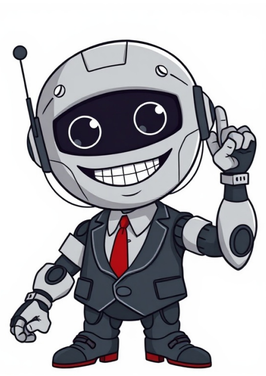
I'm not a robot



A strong password is a unique password. A good password should be made up at least 15 characters, including lowercase letters, uppercase letters, numbers, and special characters. It shouldnt include common words or sensitive information (birthdays, phone numbers).The LastPass password generator is the best way to create complex passwords, as it will create a unique password for you every time. Whether you need a new password or want to improve online security by updating old, weak passwords, you should rely on our built-in password generator. Home Blog Security Guide Test your password strength & generate secure passphrases. Generate Secure Passphrase Free Password Checker & Generator Create and test strong, secure passwords instantly. Our free online tool helps you generate unbreakable passwords and check their strengthall at zero cost. Protect your accounts with ease, forever! Your passwords are never stored or shared. Get instant password strength feedback. Easy to use, even for beginners. We respect your privacy. No ads, no tracking. "This tool helped me create the **most secure** password for my accounts!" - John D., IT Professional "The password strength checker is **super accurate**, and I love the passphrase generator!" - Emily R., Cybersecurity Enthusiast "Highly recommended for **anyone serious about online security**!" - Mark T., Web Developer Check your password strength and generate secure passphrases **for free**! Read Our Security Guide Learn the **best password security tips** to protect your accounts. Most people make these **5 password mistakes**make sure you're not one of them! Is a **strong password enough** or should you use **MFA**? Tweet Share on Facebook Share on LinkedIn What is PasswordChecker.net? + PasswordChecker.net is a free online tool that helps users check password strength and generate secure passphrases for better online security. How does the password strength checker work? + Our tool evaluates your password based on length, complexity, and common patterns to determine its strength. It also estimates how long it would take to crack the password using modern hacking techniques. Are my passwords stored? + No. PasswordChecker.net does not store or transmit any passwords. The analysis is done locally in your browser for maximum security. What is the best way to create a strong password? + A strong password should be at least 12-16 characters long, contain a mix of letters, numbers, and special characters, and avoid common words or personal information. Reusing passwords **puts all your accounts at risk**. Always use a **unique, complex password** for each account. MFA **adds an extra layer of security** by requiring a second factor (e.g., code sent to your phone). A password manager **stores and generates** strong passwords for you, so you dont have to remember them. Home Blog About Privacy FAQ Security Guide Terms Contact A Password is a secret combination of characters (letters, numbers, and symbols) used to verify your identity and grant access to a computer system, online account, or other secured resource. Passwords protect your personal information, data, and online accounts from unauthorized access. Without a strong and unique password, it becomes easier for others to gain unauthorized access and potentially steal your sensitive information or commit fraud. Therefore, keeping secure passwords confidential is essential for maintaining privacy and security in today's digital world.What is a Password?A password is a secret word or group of letters, numbers, and symbols that you use to prove who you are. It lets you access your accounts, devices, or websites safely. Only you should know your password. Passwords work like keys to a locked door. To access, you have to have the right key (password). Thus, passwords are crucial in preventing ill-motivated people from accessing your information.Long passwords that use different characters like uppercase, numerals, and symbols are considered the best passwords. This makes it difficult for them to be easily predicted by someone else. Simple passwords like password123 are dangerous. You should keep your passwords very confidential without telling anyone about it at all. If another person gets wind of your password, they will log into your accounts and cause problems.So, using secure and confidentially kept strong passwords is one way of ensuring that unauthorized persons do not gain access to personal information or online accounts.How to Create a Secure Password?Passwords are like secret codes that let you access your accounts and devices safely. Good passwords stop bad people from getting in. Companies make rules to help create strong passwords.These rules make passwords harder to guess :Use at least 8 characters, but no more than 64. Longer is better.Mix uppercase and lowercase letters.Add some numbers too.Include special symbols like! or ?.Don't use obvious words like names or birthdays. Those are easy to guess.Following these rules make your passwords strong and secure. You can also use a special password keeper app to help remember and store all your passwords safely.The most important things are using random letters, numbers, and symbols that no one else can guess, and never sharing your passwords with anyone. Doing this keeps your accounts and information protected.Examples of Strong PasswordsRelatively long passwords with a variety of characters are the most secure. To assist in creating such passwords, experts advise against using single words but instead recommend employing phrases. Thus, you take a sensible statement and create a password from it. For instance, the sentence I like to eat pizza is modified to Ili2EtPiz!123. Change some letters with figures or symbols so that they can be easily remembered.Another way is to use the first letters of every word in one long sentence and mix them with digits and symbols. Such as this: MyDogRunsFastAtTheParkEveryDay = "MrF@TPeD123?".You can also use password keeper apps to create and store tough passwords for you. Although not perfect, these are safer than reusing simple passwords everywhere. The main ideas are to use random letters, numbers, and symbols, make passwords long; and find a pattern that's unique but memorable to you. This prevents guys from guessing your passwords.How to Avoid Weak PasswordsBad people called hackers try hard to guess or steal passwords to break into accounts. With so much personal information shared online these days, hackers can easily find details about you to guess your passwords.Some common weak passwords that hackers look for include :Use the word "password" as your passwordUsing numbers in a row like 123456789Including personal details like birthdays, addresses, names of family members or petsThese types of passwords are very easy for hackers to figure out, especially if they can find personal information about you posted online. We should avoid using any passwords that contain guessable words or details about ourselves. Hackers can search social media, public records, and other sites to learn things that can help them crack impersonal passwords.How Often Should Passwords Be Changed?Just having strong passwords is not sufficient. You need to change them often, preferably every 3-6 months. The new ones have to be entirely different from their predecessors and not just a little bit changed. By doing this, it denies hackers the chance of using broken passwords over an extended period. Frequently changing into unique tough codes improves account safety with time.Alternative Methods to PasswordsInstead of using passwords, some systems now let you log in without having to remember a secret code. This is called "password period wordless" login, you get a one-time code sent to your phone or email. Just enter that code and you're logged in automatically. No password is needed.Two-step verification sends a code to your phone after you enter your password. You need both to get in.Biometrics lets you log in by scanning your fingerprint, face, or other body part instead of a password.Security keys are little devices you plug in or tap to prove it's you.One-time passwords are codes that change every time and can only be used once.Social login uses your Facebook, Google, or other account another body parts password is required.ConclusionPasswords protect your accounts from unauthorized access. Use long, random combinations of letters, numbers, and symbols that have no connection to your personal information. Change passwords frequently instead of reusing old ones. Passwordless options like biometrics and one-time codes sent to your devices are even more secure. Complex, ever-changing credentials are key to keeping your data safe from hackers. Text used for user authentication to prove identityFor other uses, see Password (disambiguation)."Passcode" redirects here. For the Japanese idol group, see Passcode (group).For assistance with your Wikipedia password, see Help:Reset password.A password field in a sign-in formA password, sometimes called a passcode, is secret data, typically a string of characters, usually used to confirm a user's identity. Traditionally, passwords were expected to be memorized,[1] but the large number of password-protected services that a typical individual accesses can make memorization of unique passwords for each service impractical.[2] Using the terminology of the NIST Digital Identity Guidelines,[3] the secret is held by a party called the claimant while the party verifying the identity of the claimant is called the verifier. When the claimant successfully demonstrates knowledge of the password to the verifier through an established authentication protocol,[4] the verifier is able to infer the claimant's identity.In general, a password is a sequence of characters including letters, digits, or other symbols. If the permissible characters are constrained to be numeric, the corresponding secret is sometimes called a personal identification number (PIN).Despite its name, a password does not need to be an actual word; indeed, a non-word (in the dictionary sense) may be harder to guess, which is a desirable property of passwords. A memorized secret consisting of a sequence of words or other text separated by spaces is sometimes called a passphrase. A passphrase is similar to a password in usage, but the former is generally longer for added security.[5]Passwords have been used since ancient times. Sentries would challenge those wishing to enter an area to supply a password or watchword, and would only allow a person or group to pass if they knew the password. Polybius describes the system for the distribution of watchwords in the Roman military as follows:The way in which they secure the passing round of the watchword for the night is as follows: from the tenth maniple of each class of infantry and cavalry, the maniple which is encamped at the lower end of the street, a man is chosen who is relieved from guard duty, and he attends every day at sunset at the tent of the tribune, and receiving from him the watchwordthat is a wooden tablet with the word inscribed on it takes his leave, and on returning to his quarters passes on the watchword and tablet before witnesses to the commander of the next maniple, who in turn passes it to the one next to him. All do the same until it reaches the first maniples, those encamped near the tents of the tribunes. These latter are obliged to deliver the tablet to the tribunes before dark. So that if all those issued are returned, the tribune knows that the watchword has been given to all the maniples, and has passed through all on its way back to him. If any one of them is missing, he makes inquiry at once, as he knows by the marks from what quarter the tablet has not returned, and whoever is responsible for the stoppage meets with the punishment he merits.[6]Passwords in military use evolved to include not just a password, but a password and a counterpassword; for example in the opening days of the Battle of Normandy, paratroopers of the U.S. 101st Airborne Division used a passwordflashwhich was presented as a challenge, and answered with the correct responsethunder. The challenge and response were changed every three days. American paratroopers also famously used a device known as a "cricket" on D-Day in place of a password system as a temporarily unique method of identification; one metallic click given by the device in lieu of a password was to be met by two clicks in reply.[7]Passwords have been used with computers since the earliest days of computing. The Compatible Time-Sharing System (CTSS), an operating system introduced at MIT in 1961, was the first computer system to implement password login.[8][9] CTSS had a LOGIN command that requested a user password. "After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy."[10] In the early 1970s, Robert Morris developed a system of storing login passwords in a hashed form as part of the Unix operating system. The system was based on a simulated Hagelin rotor crypto machine, and first appeared in 6th Edition Unix in 1974. A later version of his algorithm, known as crypt(3), used a 12-bit salt and invoked a modified form of the DES algorithm 25 times to reduce the risk of pre-computed dictionary attacks.[11]In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for multiple purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online.[12]The easier a password is for the owner to remember generally means it will be easier for an attacker to guess.[13] However, passwords that are difficult to remember may also reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password across different accounts. Similarly, the more stringent the password requirements, such as "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system.[14] Others argue longer passwords provide more security (e.g., entropy) than shorter passwords with a wide variety of characters.[15]In The Memorability and Security of Passwords,[16] Jeff Yan et al. examine the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords.Combining two or more unrelated words and altering some of the letters to special characters or numbers is another good method,[17] but a single dictionary word is not. Having a personally designed algorithm for generating obscure passwords is another good method.[18]However, asking users to remember a password consisting of a "mix of uppercase and lowercase characters" is similar to asking them to remember a sequence of bits: hard to remember, and only a little bit harder to crack (e.g. only 128 times harder to crack for 7-letter passwords, less if the user simply capitalises one of the letters). Asking users to use "both letters and digits" will often lead to easy-to-guess substitutions such as 'E' '3' and 'I' '1', substitutions that are well known to attackers. Similarly typing the password one keyboard row higher is a common trick known to attackers.[19]In 2013, Google released a list of the most common password types, all of which are considered insecure because they are too easy to guess (especially after researching an individual on social media), which includes:[20]The name of a pet, child, family member, or significant otherAnniversary dates and birthdaysBirthplaceName of a favorite holidaySomething related to a favorite sports teamThe word "password"Traditional advice to memorize passwords and never write them down has become a challenge because of the sheer number of passwords users of computers and the internet are expected to maintain. One survey concluded that the average user has around 100 passwords.[2] To manage the proliferation of passwords, some users employ the same password for multiple accounts, a dangerous practice since a data breach in one account could compromise the rest. Less risky alternatives include the use of password managers, single sign-on systems and simply keeping paper lists of less critical passwords.[21] Such practices can reduce the number of passwords that must be memorized, such as the password manager's master password, to a more manageable number.See also: Password strength and Computer securityThe security of a password-protected system depends on several factors. The overall system must be designed for sound security, with protection against computer viruses, man-in-the-middle attacks and the like. Physical security issues are also a concern, from deterring shoulder surfing to more sophisticated physical threats such as video cameras and keyboard sniffers. Passwords should be chosen so that they are hard for an attacker to guess and hard for an attacker to discover using any of the available automatic attack schemes.[22]Nowadays, it is a common practice for computer systems to hide passwords as they are typed. The purpose of this measure is to prevent bystanders from reading the password; however, some argue that this practice may lead to mistakes and stress, encouraging users to choose weak passwords. As an alternative, users should have the option to show or hide passwords as they type them.[22]Effective access control provisions may force extreme measures on criminals seeking to acquire a password or biometric token.[23] Less extreme measures include extortion, rubber hose cryptanalysis, and side channel attack.Some specific password management issues that must be considered when thinking about, choosing, and handling, a password follow.The rate at which an attacker can submit guessed passwords to the system is a key factor in determining system security. Some systems impose a time-out of several seconds after a small number (e.g., three) of failed password entry attempts, also known as throttling.[3] :63B Sec 5.2.2 In the absence of other vulnerabilities, such systems can be effectively secure with relatively simple passwords if they have been well chosen and are not easily guessed.[24]Many systems store a cryptographic hash of the password. If an attacker gets access to the file of hashed passwords guessing can be done offline, rapidly testing candidate passwords against the true password's hash value. In the example of a web-server, an online attacker can guess only at the rate at which the server will respond, while an off-line attacker (who gains access to the file) can guess at a rate limited only by the hardware on which the attack is running and the strength of the algorithm used to create the hash.Passwords that are used to generate cryptographic keys (e.g., for disk encryption or Wi-Fi security) can also be subjected to high rate guessing, known as password cracking. Lists of common passwords are widely available and can make password attacks efficient. Security in such situations depends on using passwords or passphrases of adequate complexity, making such an attack computationally infeasible for the attacker. Some systems, such as PGP and Wi-Fi WPA, apply a computation-intensive hash to the password to slow such attacks, in a technique known as key stretching.An alternative to limiting the rate at which an attacker can make guesses on a password is to limit the total number of guesses that can be made. The password can be disabled, requiring a reset, after a small number of consecutive bad guesses (say 5); and the user may be required to change the password after a larger cumulative number of bad guesses (say 30), to prevent an attacker from making an arbitrarily large number of bad guesses by interspersing them between good guesses made by the legitimate password owner.[25] Attackers may conversely use knowledge of this mitigation to implement a denial of service attack against the user by intentionally locking the user out of their own device; this denial of service may open other avenues for the attacker to manipulate the situation to their advantage via social engineering.Passwords entered into certain computer systems are saved in plaintext, which means they are not encrypted or protected in any way. The system merely compares the password entered by the user with this unprotected list when they log in. This method is extremely dangerous because anyone who manages to access the password storage can see every user's password right away. That jeopardizes every account on the system. Additionally, accounts belonging to users who have reused their passwords on other websites or services may also be compromised, which could result in a much larger security breach.More secure systems store each password in a cryptographically protected form, so access to the actual password will still be difficult for a snooper who gains internal access to the system, while validation of user access attempts remains possible. The most secure do not store passwords at all, but a one-way derivation, such as a polynomial, modulus, or an advanced hash function.[15] Roger Needham invented the now-common approach of storing only a "hashed" form of the plaintext password.[26][27] When a user types in a password on such a system, the password handling software runs through a cryptographic hash algorithm, and if the hash value generated from the user's entry matches the hash stored in the password database, the user is permitted access. The hash value is created by applying a cryptographic hash function to a string consisting of the submitted password and, in multiple implementations, another value known as a salt. A salt prevents attackers from easily building a list of hash values for common passwords and prevents password cracking efforts from scaling across all users.[28] MD5 and SHA1 are frequently used cryptographic hash functions, but they are not recommended for password hashing unless they are used as part of a larger construction such as in PBKDF2.[29]The stored datasometimes called the "password verifier" or the "password hash"is often stored in Modular Crypt Format or RFC 2307 hash format, sometimes in the /etc/passwd file or the /etc/shadow file.[30]The main storage methods for passwords are plain text, hashed, hashed and salted, and reversibly encrypted.[31] If an attacker gains access to the password file, then if it is stored as plain text, no cracking is necessary. If it is hashed but not salted then it is vulnerable to rainbow table attacks (which are more efficient than cracking). If it is reversibly encrypted then if the attacker gets the decryption key along with the file no cracking is necessary, while if he fails to get the key cracking is not possible. Thus, of the common storage formats for passwords only when passwords have been salted and hashed is cracking both necessary and possible.[31]If a cryptographic hash function is well designed, it is computationally infeasible to reverse the function to recover a plaintext password. An attacker can, however, use widely available tools to attempt to guess the passwords. These tools work by hashing possible passwords and comparing the result of each guess to the actual password hashes. If the attacker finds a match, they know that their guess is the actual password for the associated user. Password cracking tools can operate by brute force (i.e. trying every possible combination of characters) or by hashing every word from a list; large lists of possible passwords in multiple languages are widely available on the Internet.[15] The existence of password cracking tools allows attackers to easily recover poorly chosen passwords. In particular, attackers can quickly recover passwords that are short, dictionary words, simple variations on dictionary words, or that use easily guessable patterns.[32]A modified version of the DES algorithm was used as the basis for the password hashing algorithm in early Unix systems.[33] The crypt algorithm used a 12-bit salt value so that each user's hash was unique and iterated the DES algorithm 25 times in order to make the hash function slower, both measures intended to frustrate automated guessing attacks.[33] The user's password was used as a key to encrypt a fixed value. More recent Unix or Unix-like systems (e.g., Linux or the various BSD systems) use more secure password hashing algorithms such as PBKDF2, bcrypt, and scrypt, which have large salts and an adjustable cost or number of iterations.[34]A poorly designed hash function can make attacks feasible even if a strong password is chosen. LM hash is a widely deployed and insecure example.[35]Passwords are vulnerable to interception (i.e., "snooping") while being transmitted to the authenticating machine or person. If the password is carried as electrical signals on unsecured physical wiring between the user access point and the central system controlling the password database, it is subject to snooping by wiretapping methods. If it is carried as packeted data over the Internet, anyone able to watch the packets containing the logon information can snoop with a low probability of detection.Email is sometimes used to distribute passwords but this is generally an insecure method. Since most email is sent as plaintext, a message containing a password is readable without effort during transport by any eavesdropper. Further, the message will be stored as plaintext on at least two computers: the sender's and the recipient's. If it passes through intermediate systems during its travels, it will probably be stored on there as well, at least for some time, and may be copied to backup, cache or history files on any of these systems.Using client-side encryption will only protect transmission from the mail handling system server to the client machine. Previous or subsequent relays of the email will not be protected and the email will probably be stored on multiple computers, certainly on the originating and receiving computers, most often in clear text.See also: CryptographyThe risk of interception of passwords sent over the Internet can be reduced by, among other approaches, using cryptographic protection. The most widely used is the Transport Layer Security (TLS, previously called SSL) feature built into most current Internet browsers. Most browsers alert the user of a TLS/SSL-protected exchange with a server by displaying a closed lock icon, or some other sign, when TLS is in use. There are several other techniques in use.There is a conflict between stored hashed-passwords and hash-based challengeresponse authentication; the latter requires a client to prove to a server that they know what the shared secret (i.e., password) is, and to do this, the server must be able to obtain the shared secret from its stored form. On a number of systems (including Unix-type systems) doing remote authentication, the shared secret usually becomes the hashed form and has the serious limitation of exposing passwords to offline guessing attacks. In addition, when the hash is used as a shared secret, an attacker does not need the original password to authenticate remotely; they only need the hash.Rather than transmitting a password, or transmitting the hash of the password, password-authenticated key agreement systems can perform a zero-knowledge password proof, which proves knowledge of the password without exposing it.Moving a step further, augmented systems for password-authenticated key agreement (e.g., AMP, B-SPEKE, PAK-Z, SRP-6) avoid both the conflict and limitation of hash-based methods. An augmented system allows a client to prove knowledge of the password to a server, where the server knows only a (not exactly) hashed password, and where the un-hashed password is required to gain access.Main article: Self-service password resetUsually, a system must provide a way to change a password, either because a user believes the current password has been (or might have been) compromised, or as a precautionary measure. If a new password is passed to the system in unencrypted form, security can be lost (e.g., via wiretapping) before the new password can even be installed in the password database and if the new password is given to a compromised employee, little is gained. Some websites include the user-selected password in an unencrypted confirmation e-mail message, with the obvious increased vulnerability.Identity management systems are increasingly used to automate the issuance of replacements for lost passwords, a feature called self-service password reset. The user's identity is verified by asking questions and comparing the answers to ones previously stored (i.e., when the account was opened).Some password reset questions ask for personal information that could be found on social media, such as mother's maiden name. As a result, some security experts recommend either making up one's own questions or giving false answers.[36]"Password aging" is a feature of some operating systems which forces users to change passwords frequently (e.g., quarterly, monthly or even more often). Such policies usually provoke user protest and foot-dragging at best and hostility at worst.[37] There is often an increase in the number of people who note down the password and leave it where it can easily be found, as well as help desk calls to reset a forgotten password. Users may use simpler passwords or develop variation patterns on a consistent theme to keep their passwords memorable.[38] Because of these issues, there is some debate as to whether password aging is effective.[39] Changing a password will not prevent abuse in most cases, since the abuse would often be immediately noticeable. However, if someone may have had access to the password through some means, such as sharing a computer or breaching a different site, changing the password limits the window for abuse.[40]Allotting separate passwords to each user of a system is preferable to having a single password shared by legitimate users of the system, certainly from a security viewpoint. This is partly because users are more willing to tell another person (who may not be authorized) a shared password than one exclusively for their use. Single passwords are also much less convenient to change because multiple people need to be told at the same time, and they make removal of a particular user's access more difficult, as for instance on graduation or resignation. Separate logins are also often used for accountability, for example to know who changed a piece of data.Common techniques used to improve the security of computer systems protected by a password include:Not displaying the password on the display screen as it is being entered or obscuring it as it is typed by using asterisks (*) or bullets ().Allowing passwords of adequate length. (Some legacy operating systems, including early versions[which?] of Unix and Windows, limited passwords to an 8 character maximum,[41][42][43] reducing security.)Requiring users to re-enter their password after a period of inactivity (a semi log-off policy).Enforcing a password policy to increase password strength and security.Assigning randomly chosen passwords.Requiring minimum password lengths.[29]Some systems require characters from various character classes in a passwordfor example, "must have at least one uppercase and at least one lowercase letter". However, all-lowercase passwords are more secure per keystroke than mixed capitalization passwords.[44]Employ a password blacklist to block the use of weak, easily guessed passwordsProviding an alternative to keyboard entry (e.g., spoken passwords, or biometric identifiers).Requiring more than one authentication system, such as two-factor authentication (something a user has and something the user knows).Using encrypted tunnels or password-authenticated key agreement to prevent access to transmitted passwords via network attacksLimiting the number of allowed failures within a given time period (to prevent repeated password guessing). After the limit is reached, further attempts will fail (including correct password attempts) until the beginning of the next time period. However, this is vulnerable to a form of denial of service attack.Introducing a delay between password submission attempts to slow down automated password guessing programs.Some of the more stringent policy enforcement measures can pose a risk of alienating users, possibly decreasing security as a result.It is common practice amongst computer users to reuse the same password on multiple sites. This presents a substantial security risk, because an attacker needs to only compromise a single site in order to gain access to other sites the victim uses. This problem is exacerbated by also reusing usernames, and by websites requiring email logins, as it makes it easier for an attacker to track a single user across multiple sites. Password reuse can be avoided or minimized by using mnemonic techniques, writing passwords down on paper, or using a password manager.[45]It has been argued by Redmond researchers Dinei Florencio and Cormac Herley, together with Paul C. van Oorschot of Carleton University, Canada, that password reuse is inevitable, and that users should reuse passwords for low-security websites (which contain little personal data and no financial information, for example) and instead focus their efforts on remembering long, complex passwords for a few important accounts, such as bank accounts.[46] Similar arguments were made by Forbes in not change passwords as often as some "experts" advise, due to the same limitations in human memory.[38]Historically, multiple security experts asked people to memorize their passwords: "Never write down a password". More recently, multiple security experts such as Bruce Schneier recommend that people use passwords that are too complicated to memorize, write them down on paper, and keep them in a wallet.[47][48][49][50][51][52][53]Password management software can also store passwords relatively safely, in an encrypted file sealed with a single master password.[54]To facilitate estate administration, it is helpful for people to provide a mechanism for their passwords to be communicated to the persons who will administer their affairs in the event of their death. Should a record of accounts and passwords be prepared, care must be taken to ensure that the records are secure, to prevent theft or fraud.[55]Main article: Multi-factor authenticationMulti-factor authentication schemes combine passwords (as "knowledge factors") with one or more other means of authentication, to make authentication more secure and less vulnerable to compromised passwords. For example, a simple two-factor login might send a text message, e-mail, automated phone call, or similar alert whenever a login attempt is made, possibly supplying a code that must be entered in addition to a password.[56] More sophisticated factors include such things as hardware tokens and biometric security.Password rotation is a policy that is commonly implemented with the goal of enhancing computer security. In 2019, Microsoft stated that the practice is "ancient and obsolete".[57][58]Further information: Password policyMost organizations specify a password policy that sets requirements for the composition and usage of passwords, typically dictating minimum length, required categories (e.g., upper and lower case, numbers, and special characters), prohibited elements (e.g., use of one's own name, date of birth, address, telephone number). Some governments have national authentication frameworks[59] that define requirements for user authentication to government services, including requirements for passwords.Many websites enforce standard rules such as minimum and maximum length, but also frequently include composition rules such as featuring at least one capital letter and at least one number/symbol. These latter, more specific rules were largely based on a 2003 report by the National Institute of Standards and Technology (NIST), authored by Bill Burr.[60] It originally proposed the practice of using numbers, obscure characters and capital letters and updating regularly. In a 2017 article in The Wall Street Journal, Burr reported he regrets these proposals and made a mistake when he recommended them.[61]According to a 2017 rewrite of this NIST report, a number of websites have rules that actually have the opposite effect on the security of their users. This includes complex composition rules as well as forced password changes after certain periods of time. While these rules have long been widespread, they have also long been seen as annoying and ineffective by both users and cyber-security experts.[62] The NIST recommends people use longer phrases as passwords (and advises websites to raise the maximum password length) instead of hard-to-remember passwords with "illusory complexity" such as "pA55w+rd".[63] A user prevented from using the password "password" may simply choose "Password1" if required to include a number and uppercase letter. Combined with forced periodic password changes, this can lead to passwords that are difficult to remember but easy to crack.[60]Paul Grassi, one of the 2017 NIST report's authors, further elaborated: "Everyone knows that an exclamation point is a 1, or an I, or the last character of a password. $ is an S or a 5. If we use these well-known tricks, we aren't fooling any adversary. We are simply fooling the database that stores passwords into thinking the user did something good."[62]Pieris Tsokkis and Eliana Stavrou were able to identify some bad password construction strategies through their research and development of a password generator tool. They came up with eight categories of password construction strategies based on exposed password lists, password cracking tools, and online reports citing the most used passwords. These categories include user-related information, keyboard combinations and patterns, placement strategy, word processing, substitution, capitalization, append dates, and a combination of the previous categories[64]Main article: Password crackingAttempting to crack passwords by trying as many possibilities as time and money permit is a brute force attack. A related method, rather more efficient in most cases, is a dictionary attack. In a dictionary attack, all words in one or more dictionaries are tested. Lists of common passwords are also typically tested.Password strength is the likelihood that a password cannot be guessed or discovered, and varies with the attack algorithm used. Cryptologists and computer scientists often refer to the strength or 'hardness' in terms of entropy.[15]Passwords easily discovered are termed weak or vulnerable; passwords difficult or impossible to discover are considered strong. There are several programs available for password attack (or even auditing and recovery by systems personnel) such as L0phtCrack, John the Ripper, and Cain; some of which use password design vulnerabilities (as found in the Microsoft LANManager system) to increase efficiency. These programs are sometimes used by system administrators to detect weak passwords proposed by users.Studies of production computer systems have consistently shown that a large fraction of all user-chosen passwords are readily guessed automatically.[65] For example, Columbia University found 22% of user passwords could be recovered with little effort.[66] According to Bruce Schneier, examining data from a 2006 phishing attack, 55% of MySpace passwords would be crackable in 8 hours using a commercially available Password Recovery Toolkit capable of testing 200,000 passwords per second in 2006.[67] He also reported that the single most common password was password1, confirming yet again the general lack of informed care in choosing passwords among users. (He nevertheless maintained, based on these data, that the general quality of passwords has improved over the yearsfor example, average length was up to eight characters from under seven in previous surveys, and less than 4% were dictionary words.[68])On 16 July 1998, CERT reported an incident where an attacker had found 186,126 encrypted passwords. At the time the attacker was discovered, 47,642 passwords had already been cracked.[69]In September 2001, after the deaths of 658 of their 960 New York employees in the September 11 attacks, financial services firm Cantor Fitzgerald through Microsoft broke the passwords of deceased employees to gain access to files needed for servicing client accounts.[70] Technicians used brute-force attacks, and interviewers contacted families to gather personalized information that might reduce the search time for weaker passwords.[70]In December 2009, a major password breach of the Rockyou.com website occurred that led to the release of 32 million passwords. The hacker then leaked the full list of the 32 million passwords (with no other identifiable information) to the Internet. Passwords were stored in cleartext in the database and were extracted through a SQL injection vulnerability. The Imperva Application Defense Center (ADC) did an analysis on the strength of the passwords.[71]In June 2011, NATO (North Atlantic Treaty Organization) experienced a security breach that led to the public release of first and last names, usernames, and passwords for more than 11,000 registered users of their e-bookshop. The data was leaked as part of Operation AntiSec, a movement that includes Anonymous, LulzSec, as well as other hacking groups and individuals. The aim of AntiSec is to expose personal, sensitive, and restricted information to the world, using any means necessary.[72]On 11 July 2011, Booz Allen Hamilton, a consulting firm that does work for the Pentagon, had their servers hacked by Anonymous and leaked the same day. "The leak, dubbed 'Military Meltdown Monday,' includes 90,000 logins of military personnelincluding personnel from USCENTCOM, SOCOM, the Marine corps, various Air Force facilities, Homeland Security, State Department staff, and what looks like private sector contractors."[73] These leaked passwords wound up being hashed in SHA1, and were later decrypted and analyzed by the ADC team at Imperva, revealing that even military personnel look for shortcuts and ways around the password requirements.[74]On 5 June 2012, a security breach at LinkedIn resulted in 117 million stolen passwords and emails. Millions of the passwords were later posted on a Russian forum. A hacker named "Peace" later offered additional passwords for sale. LinkedIn undertook a mandatory reset of all compromised accounts.[75]The multiple ways in which permanent or semi-permanent passwords can be compromised has prompted the development of other techniques. Some are inadequate in practice, and in any case few have become universally available for users seeking a more secure alternative.[76] A 2012 paper[77] examines why passwords have proved so hard to supplant (despite multiple predictions that they would soon be a thing of the past[78]); in examining thirty representative proposed replacements with respect to security, usability and deployability they conclude "none even retains the full set of benefits that legacy passwords already provide."Single-use passwords. Having passwords that are only valid once makes a number of potential attacks ineffective. Most users find single-use passwords extremely inconvenient. They have, however, been widely implemented in personal online banking, where they are known as Transaction Authentication Numbers (TANs). As most home users only perform a small number of transactions each week, the single-use issue has not led to intolerable customer dissatisfaction in this case.Time-synchronized one-time passwords are similar in some ways to single-use passwords, but the value to be entered is displayed on a small (generally pocketable) item and changes every minute or so.Passwordless authentication which a user can log in to a computer system without entering (and having to remember) a password or any other knowledge-based secret. In most common implementations users are asked to enter their public identifier (username, phone number, email address etc.) and then complete the authentication process by providing a secure proof of identity through a registered device or token. Most of implementations rely on public-key cryptography infrastructure where the public key is provided during registration to the authenticating service (remote server, application or website) while the private key is kept on a users device (PC, smartphone or an external security token) and can be accessed only by providing a biometric signature or another authentication factor which is not knowledge-based.[79]PassWindow one-time passwords are used as single-use passwords, but the dynamic characters to be entered are visible only when a user superimposes a unique printed visual key over a server-generated challenge image shown on the user's screen.Access controls based on public-key cryptography e.g. ssh. The necessary keys are usually too large to memorize (but see proposal Passmaze)[80] and must be stored on a local computer, security token or portable memory device, such as a USB flash drive or even floppy disk. The private key may be stored on a cloud service provider, and activated by the use of a password or two-factor authentication.Biometric methods promise authentication based on unalterable personal characteristics, but as of 2008[update] have high error rates and require additional hardware to scan,[needs update] for example, fingerprints, irises, etc. They have proven easy to spoof in some famous incidents testing commercially available systems, for example, the gummie fingerprint spoof demonstration,[81] and, because these characteristics are unalterable, they cannot be changed if compromised; this is a highly important consideration in access control as a compromised access token is necessarily insecure.Single sign-on technology is claimed to eliminate the need for having multiple passwords. Such schemes do not relieve users and administrators from choosing reasonable single passwords, nor system designers or administrators from ensuring that private access control information passed among systems enabling single sign-on is secure against attack. As yet, no satisfactory standard has been developed.Envaulting technology is a password-free way to secure data on removable storage devices such as USB flash drives. Instead of user passwords, access control is based on the user's access to a network resource.Non-text-based passwords, such as graphical passwords or mouse-movement based passwords.[82] Graphical passwords are an alternative means of authentication for log-in intended to be used in place of conventional password; they use images, graphics or colours instead of letters, digits or special characters. One system requires users to select a series of faces as a password, utilizing the human brain's ability to recall faces easily.[83] In some implementations the user is required to pick from a series of images in the correct sequence in order to gain access.[84] Another graphical password solution creates a one-time password using a randomly generated grid of images. Each time the user is required to authenticate, they look for the images that fit their pre-chosen categories and enter the randomly generated alphanumeric character that appears in the image to form the one-time password.[85][86] So far, graphical passwords are promising, but are not widely used. Studies on this subject have been made to determine its usability in the real world. While some believe that graphical passwords would be harder to crack, others suggest that people will be just as likely to pick common images or sequences as they are to pick common passwords.[citation needed]2D Key (2-Dimensional Key)[87] is a 2D matrix-like key input method having the key styles of multiline passphrase, crossword, ASCII/Unicode art, with optional textual semantic noises, to create big password/key beyond 128 bits to realize the MePKC (Memorizable Public-Key Cryptography)[88] using fully memorizable private key upon the current private key management technologies like encrypted private key, split private key, and roaming private key.Cognitive passwords use question and answer cue/response pairs to verify identity."The password is dead" is a recurring idea in computer security. The reasons given often include reference to the usability as well as security problems of passwords. It often accompanies arguments that the replacement of passwords by a more secure means of authentication is both necessary and imminent. This claim has been made by a number of people at least since 2004.[89][90][91][92][93] Alternatives to passwords include biometrics, two-factor authentication or single sign-on, Microsoft's Cardspace, the Higgins project, the Liberty Alliance, NSTIC, the FIDO Alliance and various Identity 2.0 proposals.[94][95]Bonneau et al. systematically compared web passwords to other technical solutions that were alternatives. They reviewed these in respect of usability, deployability, and security. Their analysis showed that most alternatives do better than passwords on security, some do better and some worse with respect to usability, while every alternative does worse than passwords on deployability.[96]This may be why over 20 years after this recurring idea started, passwords are still being used, despite attempts by technology businesses to change this. Some that highlight this, suggest that the problem is generally not with the system of using passwords and is instead an issue with how humans use and manage their passwords and that "in the age of disparate workforces, home WiFi networks and multiple devices, password use has continued to increase".[97]Access code (disambiguation)Combination lockDicewareElectronic lockKerberos (protocol)KeyfilePassMapPassword fatiguePassword notification e-mailPassword psychologyPassword synchronizationPre-shared keyRandom password generatorShibbolethUsability of web authentication systems^ Ranjan, Pratik; Om, Hari (6 May 2016). "An Efficient Remote User Password Authentication Scheme based on Rabin's Cryptosystem". Wireless Personal Communications. 90 (1): 217244. doi:10.1007/s11277-016-3342-5. ISSN0929-6212. S2CID21912076.^ a b Williams, Shannon (21 October 2020). "Average person has 100 passwords - study". SecurityBrief New Zealand. NordPass. Retrieved 28 April 2021.^ a b Grassi, Paul A.; Garcia, Michael E.; Fenton, James L. (June 2017). "NIST Special Publication 800-63-3: Digital Identity Guidelines". National Institute of Standards and Technology (NIST). doi:10.6028/NIST.SP.800-63-3. Retrieved 17 May 2019. {{cite journal}}: Cite journal requires |journal= (help)^ "authentication protocol". Computer Security Resource Center (NIST). Archived from the original on 17 May 2019. Retrieved 17 May 2019.^ "Passphrase". Computer Security Resource Center (NIST). Retrieved 17 May 2019.^ Polybius on the Roman Military Archived 2008-02-07 at the Wayback Machine. Ancienthistory.about.com (2012-04-13). Retrieved on 2012-05-20.^ Mark Bando (2007). 101st Airborne: The Screaming Eagles in World War II. Mbi Publishing Company. ISBN978-0-7603-2984-9. Archived from the original on 2 June 2013. Retrieved 20 May 2012.^ McMillan, Robert (27 January 2012). "The World's First Computer Password? It Was Useless Too". Wired magazine. Retrieved 22 March 2019.^ Hunt, Troy (26 July 2017). "Passwords Evolved: Authentication Guidance for the Modern Era". Retrieved 22 March 2019.^ CTSS Programmers Guide, 2nd Ed., MIT Press, 1965^ Morris, Robert; Thompson, Ken (3 April 1978). "Password Security: A Case History". Bell Laboratories. CiteSeerX10.1.1.128.1635.^ "10 Uses of Passwords". 26 March 2025. Retrieved 13 November 2025.^ Vance, Ashlee (10 January 2010). "If Your Password Is 123456, Just Make It HackMe". The New York Times. Archived from the original on 11 February 2017.^ "Managing Network Security". Archived from the original on 2 March 2008. Retrieved 31 March 2009.{{cite web}}: CS1 maint: bot: original URL status unknown (link). Fred Cohen and Associates. All.net. Retrieved on 20 May 2012.^ a b c d Lundin, Leigh (11 August 2013). "PINs and Passwords, Part 2". Passwords. Orlando: SleuthSayers.^ The Memorability and Security of Passwords Archived 14 April 2012 at the Wayback Machine (pdf). ncl.ac.uk. Retrieved on 20 May 2012.^ Michael E. Whitman; Herbert J. Mattord (2014). Principles of Information Security. Cengage Learning. p.162. ISBN978-1-305-17673-7.^ "How to Create a Random Password Generator". PCMAG. Retrieved 5 September 2021.^ Lewis, Dave (2011). Ctrl-Alt-Delete. Lulu.com. p.17. ISBN978-1471019111. Retrieved 10 July 2015.^ Techlicious / Fox Van Allen @techlicious (8 August 2013). "Google Reveals the 10 Worst Password Ideas". Time. Archived from the original on 22 October 2013. Retrieved 16 October 2013.^ Fleishman, Glenn (24 November 2015). "Write your passwords down to improve safety A counter-intuitive notion leaves you less vulnerable to remote attack, not more". MacWorld. Retrieved 28 April 2021.^ a b Lyquix Blog: Do We Need to Hide Passwords? Archived 25 April 2012 at the Wayback Machine. Lyquix.com. Retrieved on 20 May 2012.^ Jonathan Kent, Malaysia car thieves steal finger . BBC (31 March 2005)^ Stuart Brown "Top ten passwords used in the United Kingdom". Archived from the original on 8 November 2006. Retrieved 14 August 2007.. Modernlifeisrubbish.co.uk (26 May 2006). Retrieved on 20 May 2012.^ US patent 8046827^ Wilkes, M. V. Time-Sharing Computer Systems. American Elsevier, New York, (1968).^ Schofield, Jack (10 March 2003). "Roger Needham". The Guardian.^ The Bug Charmer: Passwords Matter Archived 2 November 2013 at the Wayback Machine. Bugcharmer.blogspot.com (20 June 2012). Retrieved on 30 July 2013.^ a b Alexander, Steven. (20 June 2012) The Bug Charmer: How long should passwords be? Archived 20 September 2012 at the Wayback Machine. Bugcharmer.blogspot.com. Retrieved on 30 July 2013.^ "passlib.hash - Password Hashing Schemes" Archived 21 July 2013 at the Wayback Machine.^ a b Florencio et al., An Administrator's Guide to Internet Password Research Archived 14 February 2015 at the Wayback Machine. (pdf) Retrieved on 14 March 2015.^ Cracking Story How I Cracked Over 122 Million SHA1 and MD5 Hashed Passwords Thireus' Bl0g Archived 30 August 2012 at the Wayback Machine. Blog.thireus.com (29 August 2012). Retrieved on 30 July 2013.^ a b Morris, Robert & Thompson, Ken (1979). "Password Security: A Case History". Communications of the ACM. 22 (11): 594597. CiteSeerX10.1.1.135.2097. doi:10.1145/359168.359172. S2CID207656012. Archived from the original on 22 March 2003.^ Password Protection for Modern Operating Systems Archived 11 March 2016 at the Wayback Machine (pdf). Usenix.org. Retrieved on 20 May 2012.^ How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases Archived 9 May 2006 at the Wayback Machine. support.microsoft.com (3 December 2007). Retrieved on 20 May 2012.^ "Why You Should Lie When Setting Up Password Security Questions". Techlicious. 8 March 2013. Archived from the original on 23 October 2013. Retrieved 16 October 2013.^ Shay, R.; Komanduri, S.; Kelley, P. G.; Leon, P. G.; Mazurek, M. L.; Bauer, L.; Cranor, L. F. (2010). "Encountering stronger password requirements: user attitudes and behaviors". Proceedings of the Sixth Symposium on Usable Privacy and Security. pp.120. doi:10.1145/1837110.1837113. Retrieved 30 April 2025.^ a b Joseph Steinberg (12 November 2014). "Forbes: Why You Should Ignore Everything You Have Been Told About Choosing Passwords". Forbes. Archived from the original on 12 November 2014. Retrieved 12 November 2014.^ "The problems with forcing regular password expiry". IA Matters. CESG: the Information Security Arm of GCHQ. 15 April 2016. Archived from the original on 17 August 2016. Retrieved 5 August 2016.^ Schneier on Security discussion on changing passwords Archived 30 December 2010 at the Wayback Machine. Schneier.com. Retrieved on 20 May 2012.^ Seltzer, Larry. (9 February 2010) "American Express: Strong Credit, Weak Passwords" Archived 12 July 2017 at the Wayback Machine. Pcmag.com. Retrieved on 20 May 2012.^ "Ten Windows Password Myths": "NT dialog boxes ... limited passwords to a maximum of 14 characters"^ "You must provide a password between 1 and 8 characters in length". Jira.codehaus.org. Retrieved on 20 May 2012. Archived 21 May 2015 at the Wayback Machine^ "To Capitalize or Not to Capitalize?" Archived 17 February 2009 at the Wayback Machine. World.std.com. Retrieved on 20 May 2012.^ Thomas, Keir (10 February 2011). "Password Reuse Is All Too Common, Research Shows". PC World. Archived from the original on 12 August 2014. Retrieved 10 August 2014.^ Pauli, Darren (16 July 2014). "Microsoft: You NEED bad passwords and should re-use them a lot". The Register. Archived from the original on 12 August 2014. Retrieved 10 August 2014.^ Bruce Schneier: Crypto-Gram Newsletter Archived 15 November 2011 at the Wayback Machine 15 May 2001^ "Ten Windows Password Myths": Myth #7. You Should Never Write Down Your Password^ Kotadia, Munir (23 May 2005) Microsoft security guru: Jot down your passwords. News.cnet.com. Retrieved on 20 May 2012.^ "The Strong Password Dilemma" Archived 18 July 2010 at the Wayback Machine by Richard E. Smith: "we can summarize classical password selection rules as follows:The password must be impossible to remember and never written down."^ Bob Jenkins (11 January 2013). "Choosing Random Passwords". Archived from the original on 18 September 2010.^ "The Memorability and Security of Passwords Some Empirical Results" Archived 19 February 2011 at the Wayback Machine (pdf)"your password ... in a secure place, such as the back of your wallet or purse."^ "Should I write down my passphrase?" Archived 17 February 2009 at the Wayback Machine. World.std.com. Retrieved on 20 May 2012.^ "The Best Free Password Managers of 2025: Secure Your Credentials". TechRadar. 27 July 2022. Retrieved 13 November 2025.^ Redding, David E.; Features, AEP published in (19 April 2019). "Your Estate Could Have a Serious Password Problem". Kiplinger.com. Retrieved 17 August 2024.^ Two-factor authentication Archived 18 June 2016 at the Wayback Machine^ Goodin, Dan (3 June 2019). "Microsoft says mandatory password changing is "ancient and obsolete"". Ars Technica. Retrieved 1 November 2022.^ Kristen Ranta-Haikal Wilson (9 March 2020). "The Debate Around Password Rotation Policies". SANS Institute. Retrieved 31 October 2022.^ AlFayyadh, Bander; Thorsheim, Per; Jsang, Audun; Klevjer, Henning. "Improving Usability of Password Management with Standardized Password Policies" (PDF). Archived (PDF) from the original on 20 June 2013. Retrieved 12 October 2012.^ a b Tung, Liam (9 August 2017). "Hate silly password rules? So does the guy who created them". ZDNet. Archived from the original on 29 March 2018.^ McMillan, Robert (7 August 2017). "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!". The Wall Street Journal. Archived from the original on 9 August 2017.^ a b Roberts, Jeff John (11 May 2017). "Experts Say We Can Finally Ditch Those Stupid Password Rules". Fortune. Archived from the original on 28 June 2018.^ Wisniewski, Chester (18 August 2016). "NIST's new password rules what you need to know". Naked Security. Archived from the original on 28 June 2018.^ P. Tsokkis and E. Stavrou, "A password generator tool to increase users' awareness on bad password construction strategies", 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, 2018, pp. 1-5, doi:10.1109/ISNCC.2018.8531061.^ Morris, R.; Thompson, K. (1979). "Password Security: A Case History" (PDF). Communications of the ACM. 22 (11): 594597. doi:10.1145/359168.359172. Retrieved 30 April 2025.^ "Password". Archived from the original on 23 April 2007. Retrieved 20 May 2012.{{cite web}}: CS1 maint: bot: original URL status unknown (link). cs.columbia.edu^ Schneier, Real-World Passwords Archived 23 September 2008 at the Wayback Machine. Schneier.com. Retrieved on 20 May 2012.^ MySpace Passwords Aren't So Dumb Archived 29 March 2014 at the Wayback Machine. Wired.com (27 October 2006). Retrieved on 20 May 2012.^ "CERT IN-98.03". 16 July 1998. Archived from the original on 16 October 2009. Retrieved 9 September 2009.^ a b Urbina, Ian; Davis, Leslye (23 November 2014). "The Secret Life of Passwords". The New York Times. Archived from the original on 28 November 2014.^ "Consumer Password Worst Practices (pdf)" (PDF). Archived (PDF) from the original on 28 July 2011.^ "NATO site hacked". The Register. 24 June 2011. Archived from the original on 29 June 2011. Retrieved 24 July 2011.^ Biddle, Sam (11 July 2011). "Anonymous Leaks 90,000 Military Email Accounts in Latest Antisec Attack". Gizmodo. Archived from the original on 14 July 2017.^ "Military Password Analysis". 12 July 2011. Archived from the original on 15 July 2011.^ "2012 Linkedin Breach had 117 Million Emails and Passwords Stolen, Not 6.5M - Security News". www.trendmicro.com. 18 May 2016. Retrieved 11 October 2023.^ "The top 12 password-cracking techniques used by hackers". IT PRO. 14 October 2019. Retrieved 18 July 2022.^ "The Quest to Replace Passwords (pdf)" (PDF). IEEE. 15 May 2012. Archived (PDF) from the original on 19 March 2015. Retrieved 11 March 2015.^ "Gates predicts death of the password". CNET. 25 February 2004. Archived from the original on 2 April 2015. Retrieved 14 March 2015.^ "No password for Microsoft Account: What does passwordless authentication mean?". Business Today. Retrieved 12 April 2022.^ Cryptology ePrint Archive: Report 2005/434 Archived 14 June 2006 at the Wayback Machine. eprint.iacr.org. Retrieved on 20 May 2012.^ T Matsumoto. H Matsumotot; K Yamada & S Hoshino (2002). Van Renesse, Rudolf L. (ed.). "Impact of artificial 'Gummy' Fingers on Fingerprint Systems". Proc SPIE. Optical Security and Counterfeit Deterrence Techniques IV. 4677: 275. Bibcode:2002SPIE.4677..275M. doi:10.1117/12.462719. S2CID16897825.^ Using AJAX for Image Passwords AJAX Security Part 1 of 3 Archived 16 June 2006 at the Wayback Machine. waelchatila.com (18 September 2005). Retrieved on 20 May 2012.^ Butler, Rick A. (21 December 2004) Face in the Crowd Archived 27 June 2006 at the Wayback Machine. mcpmag.com. Retrieved on 20 May 2012.^ graphical password or graphical user authentication (GUA) Archived 21 February 2009 at the Wayback Machine. searchsecurity.techtarget.com. Retrieved on 20 May 2012.^ Ericka Chickowski (3 November 2010). "Images Could Change the Authentication Picture". Dark Reading. Archived from the original on 10 November 2010.^ "Confident Technologies Delivers Image-Based, Multifactor Authentication to Strengthen Passwords on Public-Facing Websites". 28 October 2010. Archived from the original on 7 November 2010.^ User Manual for 2-Dimensional Key (2D Key) Input Method and System Archived 18 July 2011 at the Wayback Machine. xpreeli.com. (8 September 2008) . Retrieved on 20 May 2012.^ Kok-Wah Lee "Methods and Systems to Create Big Memorizable Secrets and Their Applications" Patent US20110055585, WO2010010430. Filing date: 18 December 2008^ Kotadia, Munir (25 February 2004). "Gates predicts death of the password". ZDNet. Retrieved 8 May 2019.^ "IBM Reveals Five Innovations That Will Change Our Lives within Five Years". IBM. 19 December 2011. Archived from the original on 17 March 2015. Retrieved 14 March 2015.^ "Google security exec: 'Passwords are dead'". CNET. 25 February 2004. Archived from the original on 2 April 2015. Retrieved 14 March 2015.^ "Authentciation at Scale". IEEE. 25 January 2013. Archived from the original on 2 April 2015. Retrieved 12 March 2015.^ Mims, Christopher (14 July 2014). "The Password Is Finally Dying. Here's Mine". The Wall Street Journal. Archived from the original on 13 March 2015. Retrieved 14 March 2015.^ "NSTIC head Jeremy Grant wants to kill passwords". FedScoop. 14 September 2014. Archived from the original on 18 March 2015. Retrieved 14 March 2015.^ "Specifications Overview". FIDO Alliance. 25 February 2014. Archived from the original on 15 March 2015. Retrieved 15 March 2015.^ Bonneau, Joseph; Herley, Cormac; Oorschot, Paul C. van; Stajano, Frank (May 2012). "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". 2012 IEEE Symposium on Security and Privacy: 553567. doi:10.1109/SP.2012.44.^ Lurey, Craig (9 June 2022). "Why the Password Is Not Dead". Infosecurity Magazine. Retrieved 13 November 2025.Graphical Passwords: A SurveyLarge list of commonly used passwordsLarge collection of statistics about passwordsResearch Papers on Password-based CryptographyThe international passwords conferenceProcedural Advice for Organisations and Administrators (PDF)Centre for Security, Communications and Network Research, University of Plymouth (PDF)2017 draft update to NIST password standards for the U.S. federal governmentRetrieved from "2Type of matrix barcodeA QR code for the URL of the English Wikipedia Mobile main pageA QR code, short for quick-response code,[1] is a type of two-dimensional matrix barcode invented in 1994 by Masahiro Hara of the Japanese company Denso Wave for labelling automobile parts.[2][3] It features black squares on a white background with fiducial markers, readable by imaging devices like cameras, and processed using ReedSolomon error correction until the image can be appropriately interpreted. The required data is then extracted from patterns that are present in both the horizontal and the vertical components of the QR image.[4]Whereas a barcode is a machine-readable optical image that contains information specific to the labeled item, the QR code contains the data for a locator, an identifier, and web tracking. To store data efficiently, QR codes use four standardized modes of encoding: numeric, alphanumeric, byte or binary, and kanji.[5]Compared to standard UPC barcodes, the QR labeling system was applied beyond the automobile industry because of faster reading of the optical image and greater data-storage capacity in applications such as product tracking, item identification, time tracking, document management, and general marketing.[4]Demo of printing a QR codeThe QR code system was invented in 1994, at the Denso Wave automotive products company in Japan.[6][7][8] The initial alternating-square design presented by the team of researchers, headed by Masahiro Hara, was influenced by the black counters and the white counters played on a Go board;[9] the pattern of the position detection markers was determined by finding the least-used sequence of alternating black-white areas on printed matter, which was found to be (1:1:3:1:1).[10][6] The functional purpose of the QR code system was to facilitate keeping track of the types and numbers of automobile parts, by replacing individually-scanned bar-code labels on each box of auto parts with a single label that contained the data of each label. The quadrangular configuration of the QR code system consolidated the data of the various bar-code labels with kanji, kana, and alphanumeric codes printed onto a single label.[11][10][6]QR codes can be displayed on buildings, such as this one being painted in Cape Town.During June 2011, 14 million American mobile users scanned a QR code or a barcode. Some 58% of those users scanned a QR or barcode from their homes, while 39% scanned from retail stores; 53% of the 14 million users were men between the ages of 18 and 34.[12]In 2022, 89 million people in the United States scanned a QR code using their mobile devices, up by 26 percent compared to 2020. The majority of QR code users used them to make payments or to access product and menu information.[13]In September 2020, a survey found that 18.8 percent of consumers in the United States and the United Kingdom strongly agreed that they had noticed an increase in QR code use since the then-active COVID-19-related restrictions had begun several months prior.[14]As of 2024,[update] QR codes are used in a much broader context, including both commercial tracking applications and convenience-oriented applications aimed at mobile phone users (termed mobile tagging). QR codes may be used to display text to the user, to open a webpage on the user's device, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), to connect to a wireless network, or to compose an email or text message. There are a great many QR code generators available as software or as online tools that are either free or require a paid subscription.[15] The QR code has become one of the most-used types of two-dimensional code.[16]Structure of a QR code (version 7), highlighting functional elementsSeveral standards cover the encoding of data as QR codes:[17]October 1997 AIM (Association for Automatic Identification and Mobility) International[18]January 1999 JIS X 0510June 2000 ISO/IEC 18004:2000 Information technology Automatic identification and data capture techniques Bar code symbology QR code (now withdrawn) Defines QR code models 1 and 2 symbols.1 September 2006 ISO/IEC 18004:2006 Information technology Automatic identification and data capture techniques QR Code 2005 bar code symbology specification (now withdrawn)[19] Defines QR code 2005 symbols, an extension of QR code model 2. Does not specify how to read QR code model 1 symbols, or require this for compliance.1 February 2015 ISO/IEC 18004:2015 Information Automatic identification and data capture techniques QR Code barcode symbology specification (now withdrawn) Renames the QR Code 2005 symbol to QR Code and adds clarification to some procedures and minor corrections. It was withdrawn and updated to 18004:2024 in August 2024, which optimizes encoding efficiency, improves error correction, and refines structured append functionality.[20]May 2022 ISO/IEC 23941:2022 Information technology Automatic identification and data capture techniques Rectangular Micro QR Code (rMQR) bar code symbology specification[21]Defines the requirements for Micro QR

Code.August 2024 ISO/IEC 18004:2024 Information technology Automatic identification and data capture techniques QR code bar code symbology specification[22]At the application layer, there is some variation between most of the implementations. Japan's NTT DoCoMo has established de facto standards for the encoding of URLs, contact
information, and several other data types.[23] The open-source "ZXing" project maintains a list of QR code data types.[24]A QR code printed on the packaging of a cola can, linking directly to the Pepsi website so not requiring the user to manually enter the web addressQR codes have become common in consumer advertising. Typically, a smartphone
is used as a QR code scanner, displaying the code and converting it to some useful form (such as a standard URL for a website, thereby obviating the need for a user to type it into a Web browser).QR codes have become a focus of advertising strategy to provide a way to access a brand's website more quickly than by manually entering a URL.[25][26]
Beyond mere convenience to the consumer, the importance of this capability is the belief that it increases the conversion rate: the chance that contact with the advertisement will convert to a sale. It coaxes interested prospects further down the conversion funnel with little delay or effort, bringing the viewer to the advertiser's website immediately,
whereas a longer and more targeted sales pitch may lose the viewer's interest.Although initially used to track parts in vehicle manufacturing, QR codes are used over a much wider range of applications. These include commercial tracking, warehouse stock control, entertainment and transport ticketing, product and loyalty marketing, and in-store
product labeling.[citation needed] Examples of marketing include where a company's discounted and percent discount can be captured using a QR code decoder that is a mobile app, or storing a company's information such as address and related information alongside its alpha-numeric text data as can be seen in telephone directory yellow pages.
[citation needed]QR codes may appear in very public places such as this large billboard in Japan; this one links to the sagasou.mobi websiteThey can also be used to store personal information for organizations. An example of this is the Philippines National Bureau of Investigation (NBI) where NBI clearances now come with a QR code. Many of these
applications target mobile-phone users (via mobile tagging). Users may receive text, add a vCard contact to their device, open a URL, or compose an e-mail or text message after scanning QR codes. They can generate and print their own QR codes for others to scan and use by visiting one of several pay or free QR code-generating sites or apps. Google
had an API, now deprecated, to generate QR codes,[27] and apps for scanning QR codes can be found on nearly all smartphone devices.[28]QR codes have been used and printed on train tickets in China since 2010.[29]QR codes storing addresses and URLs may appear in magazines, on signs, on buses, on business cards, or on almost any object about
which users might want information. Users with a camera phone equipped with the correct reader application can scan the image of the QR code to display text and contact information, connect to a wireless network, or open a web page in the phone's browser. This act of linking from physical world objects is termed hardlinking or object
hyperlinking. QR codes also may be linked to a location to track where a code has been scanned. Either the application that scans the QR code retrieves the geo information by using GPS and cell tower triangulation (aGPS) or the URL encoded in the QR code itself is associated with a location. In 2008, a Japanese stonemason announced plans to
engrave QR codes on gravestones, allowing visitors to view information about the deceased, and family members to keep track of visits.[30] Psychologist Richard Wiseman was one of the first authors to include QR codes in a book, in Paranormality: Why We See What Isn't There (2011).[31] Microsoft Office and LibreOffice have a functionality to insert
QR code into documents.[32][33]QR codes have been incorporated into currency. In June 2011, The Royal Dutch Mint (Koninklijke Nederlandse Munt) issued the world's first official coin with a QR code to celebrate the centenary of its current building and premises. The coin can be scanned by a smartphone and originally linked to a special website
with content about the historical event and design of the coin.[34] In 2014, the Central Bank of Nigeria issued a 100-naira banknote to commemorate its centennial, the first banknote to incorporate a QR code in its design. When scanned with an internet-enabled mobile device, the code goes to a website that tells the centenary story of Nigeria.[35]In
2015, the Central Bank of the Russian Federation issued a 100-rubles note to commemorate the annexation of Crimea by the Russian Federation.[36] It contains a QR code into its design, and when scanned with an internet-enabled mobile device, the code goes to a website that details the historical and technical background of the commemorative
note. In 2017, the Bank of Ghana issued a 5-cedis banknote to commemorate 60 years of central banking in Ghana. It contains a QR code in its design which, when scanned with an internet-enabled mobile device, goes to the official Bank of Ghana website.In September 2016, the Reserve Bank of India (RBI) launched the eponymously named
BharatQR, a common QR code jointly developed by all the four major card payment companies National Payments Corporation of India that runs RuPay cards along with Mastercard, Visa, and American Express. It will also have the capability of accepting payments on the Unified Payments Interface (UPI) platform.[37][38]QR codes are used in some
augmented reality systems to determine the positions of objects in 3-dimensional space.[11]QR codes can be used on various mobile device operating systems. While initially requiring the installation and use of third-party apps, both Android and iOS (since iOS 11[39][40]) devices can now natively scan QR codes, without requiring an external app to
be used.[41] The camera app can scan and display the kind of QR code along with the link. These devices support URL redirection, which allows QR codes to send metadata to existing applications on the device.QR codes have been used to establish "virtual stores", where a gallery of product information and QR codes is presented to the customer, e.g.
on a train station wall. The customers scan the QR codes, and the products are delivered to their homes. This use started in South Korea,[42] and Argentina,[43] but is currently expanding globally.[44] Walmart, Procter & Gamble and Woolworths have already adopted the Virtual Store concept.[45]Main article: QR code paymentQR codes can be used
to store bank account information or credit card information, or they can be specifically designed to work with particular payment provider applications. There are several trial applications of QR code payments across the world.[46][47] In developing countries including China,[48][49] India[50] QR code payment is a very popular and convenient
method of making payments. Since Alipay designed a QR code payment method in 2011,[51] mobile payment has been quickly adopted in China. As of 2018, around 83% of all payments were made via mobile payment.[52]In November 2012, QR code payments were deployed on a larger scale in the Czech Republic when an open format for payment
information exchangea Short Payment Descriptorwas introduced and endorsed by the Czech Banking Association as the official local solution for QR payments.[53][54] In 2013, the European Payment Council provided guidelines for the EPC QR code enabling SCT initiation within the Eurozone.In 2017, Singapore created a task force including
government agencies such as the Monetary Authority of Singapore and Infocomm Media Development Authority to spearhead a system for e-payments using standardized QR code specifications. These specific dimensions are specialized for Singapore.[55]The e-payment system, Singapore Quick Response Code (SGQR), essentially merges various QR
codes into one label that can be used by both parties in the payment system. This allows for various banking apps to facilitate payments between multiple customers and a merchant that displays a single QR code. The SGQR scheme is co-owned by MAS and IMDA.[56] A single SGQR label contains e-payments and combines multiple payment options.
People making purchases can scan the code and see which payment options the merchant accepts.[56]QR codes can be used to log into websites: a QR code is shown on the login page on a computer screen, and when a registered user scans it with a verified smartphone, they will automatically be logged in. Authentication is performed by the
smartphone, which contacts the server. Google deployed such a login scheme in 2012.[57]There is a system whereby a QR code can be displayed on a device such as a smartphone and used as an admission ticket.[58][59] Its use is common for J1 League and Nippon Professional Baseball tickets in Japan.[60][61] In some cases, rights can be
transferred via the Internet. In Latvia, QR codes can be scanned in Riga public transport to validate Rgas Satiksme e-tickets.[62]A sign with a QR code that links to a drinks menuRestaurants can present a QR code near the front door or at the table allowing guests to view an online menu, or even redirect them to an online ordering website or app,
allowing them to order or possibly pay for their meal without having to use a cashier or waiter. QR codes can also link to daily or weekly specials that are not printed on the standardized menus,[63] and enable the establishment to update the entire menu without needing to print copies. At table-serve restaurants, QR codes enable guests to order and
pay for their meals without a waiter involved the QR code contains the table number so servers know where to bring the food.[64] This application has grown especially since the need for social distancing during the 2020 COVID-19 pandemic prompted reduced contact between service staff and customers.[64]A QR code to automatically join a WiFi
networkBy specifying the SSID, encryption type, password/passphrase, and if the SSID is hidden or not, mobile device users can quickly scan and join networks without having to manually enter the data.[65] A MeCard-like format is supported by Android and iOS 11+.[66]Common format: WIFI:S:;T:;P:;H:;;Sample:
WIFI:S:MySSID;T:WPA;P:MyPassW0rd;;QR code tile next to the grave of Wing Commander Adrian Warburton at Durnbach War Cemetery in Gmund am Tegernsee, Germany. The code links to his Wikipedia entry.A QR code can link to an obituary and can be placed on a headstone. In 2008, Ishinokoe in Yamanashi Prefecture, Japan began to sell
tombstones with QR codes produced by IT DeSign, where the code leads to a virtual grave site of the deceased.[67][68][69] Other companies, such as Wisconsin-based Interactive Headstones, have also begun implementing QR codes into tombstones.[70] In 2014, the Jewish Cemetery of La Paz in Uruguay began implementing QR codes for
tombstones.[71]QR codes can be used to generate time-based one-time passwords for electronic authentication.QR codes have been used by various retail outlets that have loyalty programs. Sometimes these programs are accessed with an app that is loaded onto a phone and includes a process triggered by a QR code scan. The QR codes for loyalty
programs tend to be found printed on the receipt for a purchase or on the products themselves. Users in these schemes collect award points by scanning a code.Serialised QR codes have been used by brands[72] and governments[73] to let consumers, retailers and distributors verify the authenticity of the products and help with detecting counterfeit
products, as part of a brand protection program.[74] However, the security level of a regular QR code is limited since QR codes printed on original products are easily reproduced on fake products, even though the analysis of data generated as a result of QR code scanning can be used to detect counterfeiting and illicit activity.[75] A higher security
level can be attained by embedding a digital watermark or copy detection pattern into the image of the QR code. This makes the QR code more secure against counterfeiting attempts; products that display a code which is counterfeit, although valid as a QR code, can be detected by scanning the secure QR code with the appropriate app.[76]The treaty
regulating apostilles (documents bearing a seal of authenticity), has been updated to allow the issuance of digital apostilles by countries; a digital apostille is a PDF document with a cryptographic signature containing a QR code for a canonical URL of the original document, allowing users to verify the apostille from a printed version of the
document.Further information: Produce traceabilityDifferent studies have been conducted to assess the effectiveness of QR codes as a means of conveying labelling information and their use as part of a food traceability system. In a field experiment, it was found that when provided free access to a smartphone with a QR code scanning app, 52.6% of
participants would use it to access labelling information.[77] A study made in South Korea showed that consumers appreciate QR code used in food traceability system, as they provide detailed information about food, as well as information that helps them in their purchasing decision.[78] If QR codes are serialised, consumers can access a web page
showing the supply chain for each ingredient, as well as information specific to each related batch, including meat processors and manufacturers, which helps address the concerns they have about the origin of their food.[79]Two QR codes that link to German contact tracing app check-ins during the COVID-19 pandemicAfter the COVID-19 pandemic
began spreading, QR codes began to be used as a "touchless" system to display information, show menus, or provide updated consumer information, especially in the hospitality industry. Restaurants replaced paper or laminated plastic menus with QR code decals on the table, which opened an online version of the menu. This prevented the need to
dispose of single-use paper menus, or institute cleaning and sanitizing procedures for permanent menus after each use.[80] Local television stations have also begun to utilize codes on local newscasts to allow viewers quicker access to stories or information involving the pandemic, including testing and immunization scheduling websites, or for links
within stories mentioned in the newscasts overall.In Australia, patrons were required to scan QR codes at shops, clubs, supermarkets, and other service and retail establishments on entry to assist contact tracing. Singapore, Taiwan, the United Kingdom, and New Zealand used similar systems.[81]QR codes are also present on COVID-19 vaccination
certificates in places such as Canada and the EU (EU Digital COVID certificate), where they can be scanned to verify the information on the certificate.[82]Unlike the older, one-dimensional barcodes that were designed to be mechanically scanned by a narrow beam of light, a QR code is detected by a two-dimensional digital image sensor and then
digitally analyzed by a programmed processor. The processor locates the three finder patterns, each consisting of three superimposed concentric squares of differing contrast at the upper left, upper right and lower left corners of the QR code image,[83] using a smaller square (or multiple squares) near the fourth corner to normalize the image for
size, orientation, and angle of viewing. The small dots throughout the QR code are then converted to binary numbers and validated with an error-correcting algorithm.The amount of data that can be represented by a QR code symbol depends on the data type (mode, or input character set), version (1, ..., 40, indicating the overall dimensions of the
symbol, i.e. 4 version number + 17 dots on each side), and error correction level. The maximum storage capacities occur for version 40 and error correction level L (low), denoted by 40-L:[16][84]Maximum character storage capacity (40-L) Character refers to individual values of the input mode (data type).Input modeMax. charactersBits/char.Possible
characters, default encodingNumeric only7,0893130, 1, 2, 3, 4, 5, 6, 7, 8, 9Alphanumeric4,29651209, AZ (upper-case only), space, $,%, *, +, -, ., /,:Binary/byte2,9538ISO/IEC 8859-1Kanji/kana1,81713Shift JIS X 0208Here are some samples of QR codes:Version 1 (2121). Content: "Ver1"Version 2 (2525). Content: "Version 2"Version 3 (2929). Content:
"Version 3 QR Code"Version 4 (3333). Content: "Version 4 QR Code, up to 50 char"Version 10 (5757). Content: "VERSION 10 QR CODE, UP TO 174 CHAR AT H LEVEL, WITH 57X57 MODULES AND PLENTY OF ERROR CORRECTION TO GO AROUND. NOTE THAT THERE ARE ADDITIONAL TRACKING BOXES" (actually encoded in all capital
letters). (Tracking boxes are more commonly called alignment patterns.)Version 25 (117117). Content: 1,269 characters of ASCII text describing QR codesVersion 40 (177177). Content: "Version 40 QR Code can contain up to 1852 chars ..." (and followed by four paragraphs of ASCII text describing QR codes). The text refers to a QR Code with a "Level
H" error correction. Other levels provide higher capacity.Damaged but still decodable QR code, link to of a QR code with artistic embellishment that will still scan correctly thanks to error correction. When scanned, the code directs users to the artist's personal website.QR codes use ReedSolomon error correction over the finite field F 256
{\displaystyle \mathbb {F} _{256}} or GF(28), the elements of which are encoded as bytes of 8 bits; the byte b 7 b 6 b 5 b 4 b 3 b 2 b 1 b 0 {\displaystyle b_{7}b_{6}b_{5}b_{4}b_{3}b_{2}b_{1}b_{0}} with a standard numerical value i = 0 7 b i 2 i {\displaystyle \textstyle \sum _{i=0}^{7}b_{i}2^{i}} encodes the field element i = 0 7 b i i
{\displaystyle \textstyle \sum _{i=0}^{7}b_{i}\alpha ^{i}} where F 256 {\displaystyle \alpha \in \mathbb {F} _{256}} is taken to be a primitive element satisfying 8 + 4 + 3 + 2 + 1 = 0 {\displaystyle \alpha ^{8}+\alpha ^{4}+\alpha ^{3}+\alpha ^{2}+1=0} . The primitive polynomial is x 8 + x 4 + x 3 + x 2 + 1 {\displaystyle
x^{8}+x^{4}+x^{3}+x^{2}+1} , corresponding to the polynomial number 285, with initial root = 0 to obtain generator polynomials.The ReedSolomon code uses one of 37 different polynomials over F 256 {\displaystyle \mathbb {F} _{256}} , with degrees ranging from 7 to 68, depending on how many error correction bytes the code adds. It is
implied by the form of ReedSolomon used (systematic BCH view) that these polynomials are all on the form i = 0 n 1 (x i) {\textstyle \prod _{i=0}^{n-1}(x-\alpha ^{i})} . However, the rules for selecting the degree n {\displaystyle n} are specific to the QR standard.For example, the generator polynomial used for the Version 1 QR code (2121), when
7 error correction bytes are used, is: g (x) = x 7 + 87 x 6 + 229 x 5 + 146 x 4 + 149 x 3 + 238 x 2 + 102 x + 21 {\displaystyle g(x)=x^{7}+\alpha ^{87}x^{6}+\alpha ^{229}x^{5}+\alpha ^{146}x^{4}+\alpha ^{149}x^{3}+\alpha ^{238}x^{2}+\alpha ^{102}x+\alpha ^{21}} .This is obtained by multiplying the first seven terms: g (x) = (x
+ 1) (x +) (x + 2) (x + 3) (x + 4) (x + 5) (x + 6) {\displaystyle g(x)=(x+1)(x+\alpha)(x+\alpha ^{2})(x+\alpha ^{3})(x+\alpha ^{4})(x+\alpha ^{5})(x+\alpha ^{6})} .The same may also be expressed using decimal coefficients (over F 256 {\displaystyle \mathbb {F} _{256}}), as: g (x) = x 7 + 127 x 6 + 122 x 5 + 154 x 4 + 164 x 3 + 11 x 2
+ 68 x + 117 {\displaystyle g(x)=x^{7}+127x^{6}+122x^{5}+154x^{4}+164x^{3}+11x^{2}+68x+117} .The highest power of x {\displaystyle x} in the polynomial (the degree n {\displaystyle n} , of the polynomial) determines the number of error correction bytes. In this case, the degree is 7.When discussing the ReedSolomon code phase there
is some risk for confusion, in that the QR ISO/IEC standard uses the term codeword for the elements of F 256 {\displaystyle \mathbb {F} _{256}} , which with respect to the ReedSolomon code are symbols, whereas it uses the term block for what with respect to the ReedSolomon code are the codewords. The number of data versus error correction
bytes within each block depends on (i) the version (side length) of the QR symbol and (ii) the error correction level, of which there are four. The higher the error correction level, the less the storage capacity. The following table lists the approximate error correction capability at each of the four levels:Level L (Low)7% of data bytes can be
restored.Level M (Medium)15% of data bytes can be restored.Level Q (Quartile)[85]25% of data bytes can be restored.Level H (High)30% of data bytes can be restored.In larger QR symbols, the message is broken up into several ReedSolomon code blocks. The block size is chosen so that no attempt is made at correcting more than 15 errors per
block; this limits the complexity of the decoding algorithm. The code blocks are then interleaved together, making it less likely that localized damage to a QR symbol will overwhelm the capacity of any single block.The Version 1 QR symbol with level L error correction, for example, consists of a single error correction block with a total of 26 code bytes
(made of 19 message bytes and seven error correction bytes). It can correct up to 2 byte errors. Hence, this code is known as a (26,19,2) error correction code over GF(28) . It is also sometimes represented in short, as a (26,19) code.Due to error correction, it is possible to create artistic QR codes with embellishments to make them more readable or
attractive to the human eye, and to incorporate colors, logos, and other features into the QR code block; the embellishments are treated as errors, but the codes still scan correctly.[86][87]It is also possible to design artistic QR codes without reducing the error correction capacity by manipulating the underlying mathematical constructs.[88][89]
Image processing algorithms are also used to reduce errors in QR-code.[90]The format information records two things: the error correction level and the mask pattern used for the symbol. Masking is used to break up patterns in the data area that might confuse a scanner, such as large blank areas or misleading features that look like the locator
marks. The mask patterns are defined on a grid that is repeated as necessary to cover the whole symbol. Modules corresponding to the dark areas of the mask are inverted. The 5-bit format information is protected from errors with a BCH code, and two complete copies are included in each QR symbol.[4] A (15,5) triple error-correcting BCH code over
GF(24) is used, having the generator polynomial g (x) = x 10 + x 8 + x 5 + x 4 + x 2 + x + 1 {\displaystyle g(x)=x^{10}+x^{8}+x^{5}+x^{4}+x^{2}+x+1} . It can correct at most 3 bit-errors out of the 5 data bits. There are a total of 15 bits in this BCH code (10 bits are added for error correction). This 15-bit code is itself X-ORed with a fixed 15-
bit mask pattern (101010000010010) to prevent an all-zero string.To obtain the error correction (EC) bytes for a message "www.wikipedia.org", the following procedure may be carried out:The message is 17 bytes long, hence it can be encoded using a (26,19,2) Reed-Solomon code to fit in a Ver1 (2121) symbol, which has a maximum capacity of 19
bytes (for L level error correction).The generator polynomial specified for the (26,19,2) code, is: g (x) = x 7 + 127 x 6 + 122 x 5 + 154 x 4 + 164 x 3 + 11 x 2 + 68 x + 117 {\displaystyle g(x)=x^{7}+127x^{6}+122x^{5}+154x^{4}+164x^{3}+11x^{2}+68x+117} ,which may also be written in the form of a matrix of decimal coefficients:[1 127
122 154 164 11 68 117]The 17-byte long message "www.wikipedia.org" as hexadecimal coefficients (ASCII values), denoted by M1 through M17 is:[77 77 77 2E 77 69 6B 69 70 65 64 69 61 2E 6F 72 67]The encoding mode is "Byte encoding". Hence the 'Enc' field is [0100] (4 bits). The length of the above message is 17 bytes hence 'Len' field is
[00010001] (8 bits). The 'End' field is End of message marker [0000] (4 bits).The message code word (without EC bytes) is of the form:['Enc' 'Len' w w w . w i k i p e d i a . o r g 'End']Substituting the hexadecimal values, it can be expressed as:[4 11 77 77 77 2E 77 69 6B 69 70 65 64 69 61 2E 6F 72 67 0]This is rearranged as 19-byte blocks of 8 bits
each:[41 17 77 77 72 E7 76 96 B6 97 06 56 46 96 12 E6 F7 26 70]Using the procedure for Reed-Solomon systematic encoding, the 7 EC bytes obtained (E1 through E7, as shown in the symbol) which are the coefficients (in decimal) of the remainder after polynomial division are: [174 173 239 6 151 143 37]or in hexadecimal values:[AE AD EF 06 97 8F
25]These 7 EC bytes are then appended to the 19-byte message. The resulting coded message has 26 bytes (in hexadecimal):[41 17 77 77 72 E7 76 96 B6 97 06 56 46 96 12 E6 F7 26 70 AE AD EF 06 97 8F 25]Note: The bit values shown in the Ver1 QR symbol below do not match with the above values, as the symbol has been masked using a mask
pattern (001).The message dataset is placed from right to left in a zigzag pattern, as shown below. In larger symbols, this is complicated by the presence of the alignment patterns and the use of multiple interleaved error-correction blocks.Meaning of format information. In the above figure, the format information is protected by a (15,5) BCH code,
which can correct up to 3 bit errors. The total length of the code is 15 bits, of which 5 are data bits (2 EC level + 3 mask pattern) and 10 are extra bits for error correction. The format mask pattern for these 15 bits is: [101010000010010]. Note that we map the masked values directly to its meaning here, in contrast to image 4 "Levels & Masks" where
the mask pattern numbers are the result of putting the 3rd to 5th mask bit, [101], over the 3rd to 5th format info bit of the QR code.Message placement within a Ver 1 QR symbol (2121). The message is encoded using a (255,248) Reed Solomon code (shortened to (26,19) code by using "padding") that can correct up to 2 byte-errors. A total of 26 code-
words consist of 7 error-correction bytes, and 17 data bytes, in addition to the "Len" (8 bit field), "Enc" (4 bit field), and "End" (4 bit field). The symbol is capable of level L error correction. The EC level is 01(L), and mask pattern is 001. Hence the first 5 bits of the format information are 01001 (without the format mask). After masking, the 5 bits
become 11100, as seen here.Larger symbol (Ver 3, 2929) illustrating interleaved blocks. The message has 26 data bytes and is encoded using two Reed-Solomon code blocks. Each block is a (255,233) Reed Solomon code (shortened to (35,13) code), which can correct up to 11 byte-errors in a single burst, containing 13 data bytes and 22 error-
correction bytes appended to the data bytes. The two 35-byte Reed-Solomon code blocks are interleaved (resulting in a total of 70 code bytes), so it can correct up to 22 byte-errors. The symbol achieves level H error correction.The general structure of a QR encoding is as a sequence of 4 bit indicators with payload length dependent on the indicator
mode (e.g. byte encoding payload length is dependent on the first byte).[91]Mode indicatorDescriptionTypical structure '[type: sizes in bits]'1 = 0b0001Numeric[0001: 4] [Character Count Indicator: variable] [Data Bit Stream: 313 charcount]2 = 0b0010Alphanumeric[0010: 4] [Character Count Indicator: variable] [Data Bit Stream: 512
charcount]4 = 0b0100Byte encoding[0100: 4] [Character Count Indicator: variable] [Data Bit Stream: 8 charcount]8 = 0b1000Kanji encoding[1000: 4] [Character Count Indicator: variable] [Data Bit Stream: 13 charcount]3 = 0b0011Structured append[0011: 4] [Symbol Position: 4] [Total Symbols: 4] [Parity: 8]7 = 0b0111ECI[0111: 4] [ECI
Assignment number: variable]5 = 0b0101FNC1 in first position[0101: 4] [Numeric/Alphanumeric/Byte/Kanji payload: variable]9 = 0b1001FNC1 in second position[1001: 4] [Application Indicator: 8] [Numeric/Alphanumeric/Byte/Kanji payload: variable]0 = 0b0000End of message[0000: 4]Note:Character Count Indicator depends on how many
modules are in a QR code (Symbol Version).ECI Assignment number Size:8 1 bits if ECI Assignment Bitstream starts with '0'8 2 bits if ECI Assignment Bitstream starts with '10'8 3 bits if ECI Assignment Bitstream starts with '110'Four-bit indicators are used to select the encoding mode and convey other information.Encoding
modesIndicatorMeaning0001Numeric encoding (10 bits per 3 digits)0010Alphanumeric encoding (11 bits per 2 characters)0100Byte encoding (8 bits per character)1000Kanji encoding (13 bits per character)0011Structured append (used to split a message across multiple QR symbols)0111Extended Channel Interpretation (select alternate character
set or encoding)0101FNC1 in first position (see Code 128 for more information)1001FNC1 in second position0000End of message (Terminator)Encoding modes can be mixed as needed within a QR symbol. (e.g., a url with a long string of alphanumeric characters)[Mode Indicator][Mode bitstream] --> [Mode Indicator][Mode bitstream] --> etc... --
> [0000 End of message (Terminator)]After every indicator that selects an encoding mode is a length field that tells how many characters are encoded in that mode. The number of bits in the length field depends on the encoding and the symbol version.Number of bits in a length field (Character Count Indicator)EncodingVer.
1910262740Numeric101214Alphanumeric91113Byte81616Kanji81012Alphanumeric encoding mode stores a message more compactly than the byte mode can, but cannot store lower-case letters and has only a limited selection of punctuation marks, which are sufficient for rudimentary web addresses. Two characters are coded in an 11-bit value by
this formula:V = 45 C1 + C2This has the exception that the last character in an alphanumeric string with an odd length is read as a 6-bit value instead.Alphanumeric character
codesCodeCharacterCodeCharacterCodeCharacterCodeCharacterCodeCharacter00009918I27R36Space01110A19J28S37$02211B20K29T38%03312C21L30U39*04413D22M31V40+05514E23N32W41-06615F24O33X42.07716G25P34Y43/08817H26Q35Z44:The following images offer more information about the QR code.1 Introduction2 Structure3
Layout & Encoding4 Levels & Masks5 ProtocolsModel 1 QR code is an older version of the specification. It is visually similar to the widely seen model 2 codes, but lacks alignment patterns. Differences are in the bottom right corner, and in the midsections of the bottom and right edges are additional functional regions.Model 1 QR code exampleModel
1 QR code functional regionsMicro QR code is a smaller version of the QR code standard for applications where symbol size is limited. There are four different versions (sizes) of Micro QR codes: the smallest is 1111 modules; the largest can hold 35 numeric characters,[92] or 21 ASCII alphanumeric characters, or 15 bytes (120 bits).Micro QR code
exampleMicro QR code functional regionsMain article: Rectangular Micro QR CodeRectangular Micro QR Code (also known as rMQR Code) is a two-dimensional (2D) matrix barcode invented and standardized in 2022 by Denso Wave as ISO/IEC 23941. rMQR Code is designed as a rectangular variation of the QR code and has the same parameters
and applications as original QR codes; however, rMQR Code is more suitable for rectangular areas, and has a difference between width and height up to 19 in the R7x139 version.Rectangular Micro QR Code (rMQR Code) exampleiQR code is an alternative to existing square QR codes developed by Denso Wave. iQR codes can be created in square or
rectangular formations; this is intended for situations where a longer and narrower rectangular shape is more suitable, such as on cylindrical objects. iQR codes can fit the same amount of information in 30% less space. There are 61 versions of square iQR codes, and 15 versions of rectangular codes. For squares, the minimum size is 99 modules;
rectangles have a minimum of 195 modules. iQR codes add error correction level S, which allows for 50% error correction.[93] iQR Codes had not been given an ISO/IEC specification as of 2015, and only proprietary Denso Wave products could create or read iQR codes.[94]iQR code exampleSecure Quick Response Code (SQRC) is a QR code that
contains a "private data" segment after the terminator instead of the specified filler bytes "ec 11".[95] This private data segment must be deciphered with an encryption key. This can be used to store private information and to manage a company's internal information.[96]Frame QR is a variant of the QR code standard which arranges the code in a
frame around a central empty area. It is intended to be used in applications where an image, artwork, or branding is desired to be part of the code. It is a completely separate variant and is unrelated to the use of the standard QR code's error correction to insert artwork. As a variant, some QR code readers are unable to read Frame QR.[97]Frame QR
exampleFrame QR code example with a circular frame and the Wikipedia logo composed into its interiorResearchers have proposed a new High Capacity Colored 2-Dimensional (HCC2D) Code, which builds upon a QR code basis for preserving the QR robustness to distortions and uses colors for increasing data density (as of 2014 it is still in the
prototyping phase). The HCC2D code specification is described in details in Querini et al. (2011),[98] while techniques for color classification of HCC2D code cells are described in detail in Querini and Italiano (2014),[99] which is an extended version of Querini and Italiano (2013).[100]Introducing colors into QR codes requires addressing additional
issues. In particular, during QR code reading only the brightness information is taken into account, while HCC2D codes have to cope with chromatic distortions during the decoding phase. In order to ensure adaptation to chromatic distortions that arise in each scanned code, HCC2D codes make use of an additional field: the Color Palette Pattern.
This is because color cells of a Color Palette Pattern are supposed to be distorted in the same way as color cells of the Encoding Region. Replicated color palettes are used for training machine-learning classifiers.HCC2D code examples: (a) 4-color HCC2D code and (b) 8-color HCC2D codeAccessible QR (AQR) is a type of QR code that combines a
standard QR code with a dot-dash pattern positioned around one corner of the code to provide product information for people who are blind and partially sighted. The codes, announce product categories and product details such as instructions, ingredients, safety warnings, and recycling information. The data is structured for the needs of users who
are blind or partially sighted and offers larger text or audio output. It can read QR codes from a metre away, activating the smartphone's accessibility features like VoiceOver to announce product details.Further information (in Japanese): tQR code(redirect)[ja]tQR (also known as tQR code) is a QR code specially designed for rail transport to
distinguish between the different opening and closing positions of platform screen doors, which vary depending on rolling stock.[101] The initial "t" stands for "toughness" and "train".[102] It has an outer frame, and its main feature is that it can be restored even if up to 50% of data bytes is missing.[101] It was jointly developed by Denso Wave and
the Tokyo Metropolitan Bureau of Transportation.[101][103] It is stuck to the outside of the doors of rolling stock and stores the train composition number and the car number. The tQR reader installed on the platform detects the position of tQR, which allows it to detect the opening and closing of doors and the movement of rolling stock. If it is easily
readable, it could be exploited for mischiefs, so it is not compatible with existing QR codes and cannot be read by standard cameras on smartphones or other devices.[104]tQR stuck to the door of rolling stockThe use of QR code technology is freely licensed as long as users follow the standards for QR code documented with JIS or ISO/IEC. Non-
standardized codes may require special licensing.[105]Denso Wave owns a number of patents on QR code technology, but has chosen to exercise them in a limited fashion.[105] In order to promote widespread usage of the technology Denso Wave chose to waive its rights to a key patent in its possession for standardized codes only.[17] In the US, the
granted QR code patent, 5726435, expired on March 14, 2015. In Japan, the corresponding patent, 2938338, expired on March 14, 2014. The European Patent Office granted patent 0672994 to Denso Wave, which was then validated into French, UK, and German patents, all of which expired in March 2015.[106]The text QR Code itself is a registered
trademark and wordmark of Denso Wave Incorporated.[107] In UK, the trademark is registered as E921775, the term QR Code, with a filing date of 3 September 1998.[108] The UK version of the trademark is based on the Kabushiki Kaisha Denso (DENSO CORPORATION) trademark, filed as Trademark 000921775, the term QR Code, on 3 September
1998 and registered on 16 December 1999 with the European Union OHIM (Office for Harmonization in the Internal Market).[109]The U.S. Trademark for the term QR Code is Trademark 2435991 and was filed on 29 September 1998 with an amended registration date of 13 March 2001, assigned to Denso Corporation.[110] In South Korea,
trademark application filed on 18 November 2011 was refused on 20 March 2012, because the Korean Intellectual Property Office viewed that the phrase was genericized among South Korean people to refer to matrix barcodes in general.[111]The only context in which common QR codes can carry executable data is the URL data type. These URLs
may host JavaScript code, which can be used to exploit vulnerabilities in applications on the host system, such as the reader, the web browser, or the image viewer, since a reader will typically send the data to the application associated with the data type used by the QR code.In the case of no software exploits, malicious QR codes combined with a
permissive reader can still put a computer's contents and user's privacy at risk. This practice is known as "attagging", a portmanteau of "attack tagging".[112] They are easily created and can be affixed over legitimate QR codes.[113][failed verification][114] On a smartphone, the reader's permissions may allow use of the camera, full Internet access,
read/write contact data, GPS, read browser history, read/write local storage, and global system changes.[115][116][117][improper synthesis?]Risks include linking to dangerous web sites with browser exploits, enabling the microphone/camera/GPS, and then streaming those feeds to a remote server, analysis of sensitive data (passwords, files,
contacts, transactions),[118] and sending email/SMS/IM messages or packets for DDoS as part of a botnet, corrupting privacy settings, stealing identity,[119] and even containing malicious logic themselves such as JavaScript[120] or a virus.[121][122] These actions could occur in the background while the user is only seeing the reader opening a
seemingly harmless web page.[123] In Russia, a malicious QR code caused phones that scanned it to send premium texts at a fee of $6 each.[112] QR codes have also been linked to scams in which stickers are placed on parking meters and other devices, posing as quick payment options, as seen in Austin, San Antonio and Boston, among other cities
across the United States and Australia.[124][125][126]Aztec CodeData MatrixHigh Capacity Color BarcodeJAB CodeMaxiCodePDF417QRpediaSnapTagSPARQCodeTouchatag^ Hara, Masahiro (1 October 2024). "I used to hate QR codes. But they're actually genius" (Interview). Interviewed by Muller, Derek. 34:09. Retrieved 1 October 2024. The
biggest feature of QR codes is that they can be read quickly. It's called Quick Response because it reacts quickly.^ Hung, Shih-Hsuan; Yao, Chih-Yuan; Fang, Yu-Jen; Tan, Ping; Lee, RuenRone; Sheffer, Alla; Chu, Hung-Kuo (1 September 2020). "Micrography QR Codes". IEEE Transactions on Visualization and Computer Graphics. 26 (9): 28342847.
Bibcode:2020ITVCG..26.2834H. doi:10.1109/TVCG.2019.2896895. ISSN1077-2626. PMID30716038. S2CID73433883.^ Chen, Rongjun; Yu, Yongxing; Xu, Xiansheng; Wang, Leijun; Zhao, Huimin; Tan, Hong-Zhou (11 December 2019). "Adaptive Binarization of QR Code Images for Fast Automatic Sorting in Warehouse Systems". Sensors. 19 (24): 5466.
Bibcode:2019Senso..19.5466C. doi:10.3390/s19245466. PMC6960674. PMID31835866.^ a b c "QR Code Essentials". Denso ADC. 2011. Archived from the original on 12 May 2013. Retrieved 12 March 2013.^ "QR Code features". Denso-Wave. Archived from the original on 29 January 2013. Retrieved 3 October 2011.^ a b c "QR" [QR code
development]. Denso Wave (in Japanese). Archived from the original on 26 October 2021. Retrieved 26 October 2021.^ "2D Barcodes". NHK World-Japan. 26 March 2020. Archived from the original on 7 April 2020. Retrieved 7 April 2020.^ "From Japanese Auto Parts to Ubiquity: A Look at the History of QR Codes". Mainichi Daily News. 9 November
2021. Archived from the original on 11 November 2021. Retrieved 11 November 2021.^ "The Little-Known Story of the Birth of the QR Code". 10 February 2020. Archived from the original on 4 March 2020. Retrieved 4 March 2020.^ a b "History of QR Code". Denso Wave. Retrieved 30 April 2023.^ a b Furht, Borko (2011). Handbook of Augmented Reality. Springer. p.341.
ISBN9781461400646. Archived from the original on 21 December 2016.^ "14m Americans scanned QR and bar codes with their mobiles in June 2011". 16 August 2011. Archived from the original on 5 April 2016. Retrieved 27 May 2016.^ "Mobile QR scanner usage in the U.S. 2025". Statista. Retrieved 24 December 2023.^ "U.S. and UK increase of
QR code use 2020". 6 July 2021. Archived from the original on 14 August 2021. Retrieved 13 August 2021.^ Waters, Joe. "How to Use the Top QR Code Generators". Dummies.com. Archived from the original on 11 September 2017. Retrieved 5 June 2017.^ a b "QR CodeAbout 2D Code". Denso-Wave. Archived from the original on 5 June 2016.
Retrieved 27 May 2016.^ a b "QR Code Standardization". QR Code.com. Denso-Wave. Archived from the original on 10 May 2016. Retrieved 23 May 2016.^ "ISS QR Code|AIM Store: Historical Archive". Aimglobal.org. Archived from the original on 8 August 2016. Retrieved 26 May 2016.^ "ISO/IEC 18004:2006 - Information technology Automatic
identification and data capture techniques QR Code 2005 bar code symbology specification". ISO. 5 February 2009. Archived from the original on 8 March 2017. Retrieved 7 March 2017.^ "ISO/IEC 18004:2024". International Organization for Standardization. Retrieved 1 April 2025.^ "ISO/IEC 23941:2022 Information technology Automatic
identification and data capture techniques Rectangular Micro QR Code (rMQR) bar code symbology specification". ISO. Archived from the original on 3 January 2023. Retrieved 3 January 2023.^ "ISO/IEC 18004:2024". ISO. Retrieved 22 November 2025.^ "Synchronization with Native Applications". NTT DoCoMo. Archived from the original on 6
August 2016. Retrieved 26 May 2016.^ Sean Owen (17 January 2014). "Barcode contents". GitHub. Archived from the original on 15 February 2016. Retrieved 26 May 2016.^ Rimma Kats (23 January 2012). "Starbucks promotes coffee blend via QR codes". Archived from the original on 3 June 2016. Retrieved 26 May 2016.^ Jenny Lee (4 January
2012). "Tesco's cool QR code advertising campaign". Vancouversun. Archived from the original on 3 June 2016. Retrieved 26 May 2016.^ "Getting Started with Infographics (deprecated)". google-developers.appspot.com. 26 May 2015. Archived from the original on 29 June 2016. Retrieved 27 May 2016.^ "QR Code Readers for iPhone, Android,
Blackberry and Windows Phone 7". 7 December 2010. Archived from the original on 25 August 2011.^ "QR codes on China's train tickets may leak personal information". Want China Times. Archived from the original on 12 December 2013. Retrieved 16 March 2013.^ Novak, Asami (23 March 2008). "Japanese Gravestones Memorialize the Dead With
QR Codes". Wired. Archived from the original on 15 February 2013. Retrieved 8 May 2013.^ Skepticality (16 August 2011). "Paranormality: Why we see what isn't there". theguardian.com. Retrieved 13 September 2025.^ "Field codes: DisplayBarcode". Microsoft Support. Retrieved 22 April 2023.^ "LibreOffice 6.4: Release Notes". The Document
Foundation Wiki. Retrieved 22 April 2023.^ "Herdenkingsmunt met QR code volop in het nieuws!" [Commemorative QR code in the news!]. Koninklijke Nederlandse Munt (in Dutch). 21 June 2011. Archived from the original on 29 June 2016. Retrieved 27 May 2016.^ "New 100 Commemorative Centenary Celebration". Archived from the original on 8
September 2015. Retrieved 10 September 2015.^ "Russia Marks Crimea Annexation With A Banknote Rapidly Losing Value". NPR. 23 December 2015. Archived from the original on 23 December 2015. Retrieved 20 June 2024.^ "With IndiaQR launch, retail payments to get digital edge". ET Retail. Archived from the original on 15 February 2017.
Retrieved 15 February 2017.^ "IndiaQR to debut on Feb 20". The Times of India. Archived from the original on 16 February 2017. Retrieved 15 February 2017.^ "Apple hid a QR Code scanner in iOS 11 here's how to use it". CNET. Retrieved 1 October 2024.^ Lopez, Napier (7 June 2017). "iOS 11 makes QR codes cool again". TNW | Apple. Retrieved
1 October 2024.^ Lacoma, Tyler (3 October 2018). "How to Scan a QR Code". Digital Trends. Archived from the original on 22 April 2019. Retrieved 28 May 2019.^ "Tesco QR Code Virtual Store". 14 April 2012. Archived from the original on 25 May 2016. Retrieved 26 May 2016.^ Sebastin Campanario (16 September 2011). "Marketing futurista: ya
se puede comprar con la cmara del celular" [Futuristic marketing: it's already possible to purchase with a cellphone's camera]. Clarin.com (in Spanish). Archived from the original on 23 September 2011.^ "Marketers scatter phone-friendly codes across ads". 11 November 2010. Archived from the original on 12 January 2023. Retrieved 26 May 2016.^
"Top 10 QR Code Store examples". 14 April 2012. Archived from the original on 6 June 2016. Retrieved 26 May 2016.^ "SCVNGR Unveils QR Code Payment System". Mashable. 12 October 2011. Archived from the original on 8 December 2012.^ Kim, Ryan (26 January 2012). "MasterCard starts piloting QkR mobile payment app". Gigaom. Archived
from the original on 8 January 2014.^ Jacobs, Harrison. "One photo shows that China is already in a cashless future". Business Insider. Archived from the original on 5 May 2019. Retrieved 14 October 2019.^ Mozur, Paul (16 July 2017). "In Urban China, Cash Is Rapidly Becoming Obsolete". The New York Times. ISSN0362-4331. Archived from the
original on 21 October 2019. Retrieved 14 October 2019.^ "Paying With Your Mobile Wallet To Get Simpler With Interoperable QR Codes". Moneycontrol. 28 October 2020. Archived from the original on 1 November 2020. Retrieved 22 December 2020.^ "A Hangzhou Story: The Development of China's Mobile Payment Revolution" (PDF). Archived
(PDF) from the original on 26 June 2020. Retrieved 23 June 2020.^ "Payment methods in China: How China became a mobile-first nation". Daxue Consulting. Archived from the original on 29 June 2020. Retrieved 23 June 2020.^ "Standard - Formt pro sdlen platebnch daj v rmci tuzemskho platebnho styku v CZK prostednictvm QR kd" [Standard No.
26: Format for exchanging payment information for domestic payments in CZK using QR codes] (in Czech). Czech Banking Association. November 2012. Archived from the original on 3 June 2016. Retrieved 27 May 2016.^ "Formt pro sdlen platebnch daj v CZK - QR kdy" [Format for exchanging payment information in CZK - QR codes] (in Czech).
Czech Banking Association. August 2015. Archived from the original on 2020-02-16. Retrieved 2020-02-17.^ IMDA (9 November 2022). "Annex A Fact sheet on Singapore Quick Response Code (SGQR)" (PDF). Archived (PDF) from the original on 5 December 2022. Retrieved 10 November 2022.^ a b Monetary Authority of Singapore (9 November
2022). "Singapore Quick Response Code (SGQR)". Archived from the original on 26 July 2022. Retrieved 10 November 2022.^ Naraine, Ryan (17 January 2012). "Google testing login authentication via QR codes". ZDNet. Archived from the original on 15 June 2013.^ " " (in Japanese). Archived from the original on 20 October 2022. Retrieved 20
October 2022.^ "QRUSJ WEB". USJ (in Japanese). Archived from the original on 20 October 2022. Retrieved 20 October 2022.^ "QR". (in Japanese). 6 June 2025.^ "". (in Japanese). Archived from the original on 20 October 2022. Retrieved 20 October 2022.^ "New Riga public transport tickets are on sale now | Rgas valstspilstas pavaldba". riga.lv.
Retrieved 13 September 2023.^ "The Business of Eating & Restaurant Management News". Modern Restaurant Management. 22 October 2020. Archived from the original on 1 November 2020. Retrieved 1 November 2020.^ a b Kastrenakes, Jacob (29 September 2020). "Square launches QR codes that let you order from your table at a restaurant".
Verge.com. VOX Media LLC. Archived from the original on 23 November 2020. Retrieved 24 November 2020.^ Bhattacharjee, Mrinmay (19 July 2015). "Share your Wi-Fi SSID & Password using a QR Code". Technostarry. Archived from the original on 12 January 2023. Retrieved 6 January 2018.^ "zxing documentation: barcode contents". GitHub.
zxing. Archived from the original on 15 February 2016. Retrieved 26 May 2016.^ "". Archived from the original on 13 November 2015. Retrieved 10 September 2015.^ Michael Keferl (20 March 2008). "QR code graves give a "Memorial Window"". Japan Trends. Archived from the original on 2 May 2012.^ " - " (in Japanese). Archived from the original
on 13 November 2015. Retrieved 10 September 2015.^ "Quiring Monuments adds smartphone codes to gravestones". Puget Sound Business Journal. 26 April 2011. Archived from the original on 23 June 2015. Retrieved 10 September 2015.^ "Uruguayan Jewish Cemetery QR-ified" (in Spanish). EL PAIS. 24 March 2014. Archived from the original on 3
August 2016.^ "Exclusive - CHINA: Pernod Ricard to use QR codes on all China packaging". just-drinks.com. 17 September 2013. Retrieved 24 April 2020.^ "Digital tax stamps will curb fake goods - URA". Daily Monitor. Archived from the original on 12 January 2023. Retrieved 24 April 2020.^ "The power of smart packaging". bakingbusiness.com.
Archived from the original on 12 January 2023. Retrieved 3 May 2020.^ Baldini, Gianmarco; Nai Fovino, Igor; Satta, Riccardo; Tsois, Aris; Checchi, Enrico (2015). Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement. Luxembourg: European Commission. Joint Research Centre, Publications
Office. pp.28, 8992. ISBN978-92-79-54543-6. OCLC948769705.^ Carron, Cecilia (6 May 2015). "Combatting counterfeiting using QR codes". phys.org. Archived from the original on 12 January 2023. Retrieved 16 June 2020.^ Li, Tongzhe; Messer, Kent D.; Li, Tongzhe; Messer, Kent D. (2019). Li, Tongzhe; Messer, Kent D. (eds.). "To Scan or Not to
Scan: The Question of Consumer Behavior and QR Codes on Food Packages". Journal of Agricultural and Resource Economics. 44 (2): 311327. doi:10.22004/ag.econ.287977. ISSN1068-5502. Archived from the original on 1 November 2020. Retrieved 24 June 2020.^ Kim, Yeong Gug; Woo, Eunju (1 July 2016). "Consumer acceptance of a quick
response (QR) code for the food traceability system: Application of an extended technology acceptance model (TAM)". Food Research International. 85: 266272. doi:10.1016/j.foodres.2016.05.002. ISSN0963-9969. PMID29544844.^ "Behind Every Smart Product is Smart Packaging | Future Food Asia". futurefoodasia.com. Archived from the original
on 21 June 2020. Retrieved 24 June 2020.^ Leger, Benjamin (27 October 2020). "QR codes are replacing physical menus at restaurants". [225]. Archived from the original on 1 November 2020. Retrieved 1 November 2020.^ Purtill, James (19 November 2020). "The proliferation of QR code check-ins is a 'dog's breakfast'. Is there a better way?".
Australian Broadcasting Corporation. Archived from the original on 30 January 2021. Retrieved 15 January 2021.^ Hristova, Bobby (28 December 2021). "Ontarians need QR code to prove vaccination next week. Here's what you need to know". Archived from the original on 31 December 2021. Retrieved 30 December 2021.^ "ISO/IEC 18004:2024(en)
- QR code bar code symbology specification". International Organization for Standardization. Archived from the original on 20 June 2025. Retrieved 22 June 2025.^ "Information capacity and versions of QR Code". Denso-Wave. Archived from the original on 29 May 2016.^ "2D Barcode: QR-Code". Archived from the original on 15 September 2012.
TEC-IT^ Hamilton Chan (18 April 2011). "HOW TO: Make Your QR Codes More Beautiful". Mashable. Archived from the original on 10 July 2012. Retrieved 29 July 2011.^ Orli Sharaby (18 October 2010). "Form Meets Function: Extreme Makeover QR Code Edition". Archived from the original on 8 July 2012. Retrieved 29 July 2011.^ Russ Cox (12
April 2012). "QArt Codes: How to make pictures with QR codes, part II". Archived from the original on 21 March 2015. Retrieved 8 May 2015.^ Russ Cox (12 April 2012). "QArt Coder". Archived from the original on 24 April 2015. Retrieved 8 May 2015.^ Gupta, Kishor Datta; Ahsan, Md Manjurul; Andrei, Stefan (January 2018). "Extending the Storage
Capacity And Noise Reduction of a Faster QR-Code". Brain Broad Research in Artificial Intelligence and Neuroscience. 9 (1): 5971.^ ISO/IEC 18004:2006(E) 6.4 Data encoding; Table 3 Number of bits in character count indicator for QR code 2005^ Information technology Automatic identification and data capture techniques QR Code 2005 bar code
symbology specification, ISO/IEC 18004:2006 cor. 2009, pages 3, 6.^ "QR Code Overview & Progress of QR Code Applications" (PDF). Archived (PDF) from the original on 20 May 2013. Retrieved 26 June 2014.^ "iQR Code QRcode.com DENSO WAVE". Archived from the original on 7 September 2015. Retrieved 10 September 2015.^ "Embedding
Secret Data in QR Code". Archived from the original on 30 October 2018. Retrieved 29 October 2018.^ "SQRC". qrcode.com. Archived from the original on 1 January 2018. Retrieved 26 December 2017.^ "Frame QR". qrcode.com. Archived from the original on 20 December 2017. Retrieved 26 December 2017.^ Querini, M; Grillo, A; Lentini, A;
Italiano, GF (2011). "2D Color Barcodes for Mobile Phones" (PDF). International Journal of Computer Science and Applications. 8 (1). Technomathematics Research Foundation: 136155. Archived from the original (PDF) on 4 March 2016. Retrieved 21 December 2024.^ Querini, Marco; Italiano, Giuseppi F (2014). "Reliability and Data Density in High
Capacity Color Barcodes" (PDF). Computer Science and Information Systems. 11 (4): 15951615. doi:10.2298/CSIS131218054Q. Archived from the original (PDF) on 24 July 2015. Retrieved 21 December 2024.^ Querini, Marco; Italiano, Giuseppi F (2013). "Color classifiers for 2D color barcodes" (PDF). Federated Conference on Computer Science and
Information System. Archived from the original (PDF) on 24 July 2015.^ a b c " QRDENSOWAVE". www.denso-wave.com (in Japanese). 3 October 2019. Archived from the original on 20 June 2025. Retrieved 10 October 2025.^ , ; , (15 December 2023). "QR". (in Japanese). Archived from the original on 14 August 2025. Retrieved 10 October 2025.^
"QR100". (in Japanese). 21 December 2023. Archived from the original on 14 January 2025. Retrieved 10 October 2025.^ , (22 December 2020). "QR 1/2". (in Japanese). Archived from the original on 10 October 2025. Retrieved 10 October 2025.^ a b "About the patent". Denso-Wave. Archived from the original on 25 June 2016. Retrieved 26 June
2016.^ "DPA". Archived from the original on 26 July 2018. Retrieved 28 July 2016."INPI". Archived from the original on 13 August 2016."UK IPO". 9 March 2013. Archived from the original on 14 June 2019. Retrieved 28 July 2016.^ "QR Code.com". Denso-Wave. 6 November 2003. Archived from the original on 15 September 2012. Retrieved 23 April
2009.^ "UK QR Code Trademark". Archived from the original on 15 September 2012.^ "EU QR Code Trademark". Archived from the original on 15 September 2012.^ "US QR Code Trademark". Archived from the original on 15 September 2012.^ "KR QR Code Trademark Application". 2010. doi:10.8080/4020100059499. Archived from the original on
18 November 2023.^ a b "Jargon Watch", Wired, vol.20, no.1, p.22, January 2012.^ "Malicious Images: What's a QR Code". SANS Technology Institute. 3 August 2011. Archived from the original on 13 July 2012. Retrieved 31 August 2011.^ Waqas, Iam (19 October 2021). "Risks of Using QR Codes and How To Mitigate it Not As Safe as You Think".
Institute of Electrical and Electronics Engineers (IEEE). Retrieved 21 October 2024.^ "Barcode Scanner". 1 June 2011. Archived from the original on 15 September 2012. Retrieved 31 August 2011.^ "QR Droid". 19 August 2011. Archived from the original on 15 September 2012. Retrieved 31 August 2011.^ "ScanLife Barcode Reader". 24 May 2011.
Archived from the original on 15 September 2012. Retrieved 31 August 2011.^ "Consumer Alert: QR Code Safety". Better Business Bureau. 23 June 2011. Archived from the original on 15 July 2012. Retrieved 31 August 2011.^ "AVG Cautions: Beware of Malicious QR Codes". PC World. 28 June 2011. Archived from the original on 7 September 2012.
Retrieved 31 August 2011.^ "EvilQR When QRCode goes bad". AppSec-Labs Blog. 14 August 2011. Archived from the original on 15 September 2012. Retrieved 31 August 2011.^ "QR Codes: A Recipe for a Mobile Malware Tsunami". Cyveillance, Inc. 20 October 2010. Archived from the original on 28 July 2012. Retrieved 31 August 2011.^ QR codes
hold up to 2.9 KB whereas the smallest known computer virus is about one-tenth that size "The Smallest Virus I Could Manage". Virus Labs and Distribution. 1995. Archived from the original on 15 September 2012. Retrieved 31 August 2011.^ "Beware of Malicious QR Codes". ABC. 8 June 2011. Archived from the original on 1 August 2012. Retrieved
31 August 2011.^ Binder, Matt. "Beware the QR code scams". Mashable. Archived from the original on 17 January 2022. Retrieved 18 January 2022.^ Vincent, James (12 January 2022). "The latest phishing scam to watch out for: fraudulent QR codes on parking meters". The Verge. Archived from the original on 17 January 2022. Retrieved 18 January
2022.^ Wodinsky, Shoshana (12 January 2022). "Scammers Are Using QR Codes to Plunder Parking Meter Payments". Gizmodo. Archived from the original on 18 January 2022. Retrieved 18 January 2022.BS ISO/IEC 18004:2006. Information technology. Automatic identification and data capture techniques. Bar code symbology. QR Code. Geneva:
ISO/IEC. 2000. p.114. OCLC60816353.BS ISO/IEC 18004:2006. Information technology. Automatic identification and data capture techniques. QR Code 2005 bar code symbology specification. London: BSI. 2007. p.126. ISBN978-0-580-67368-9. Retrieved 4 May 2023.Wikimedia Commons has media related to QR codes.Reed Solomon Codes for Coders
an elaborate tutorial on Wikiversity, covering both QR code structure and the Reed Solomon codes used to encode the data.Retrieved from " the slider or input field to set your desired password length. Toggle the checkboxes to include or exclude uppercase letters, lowercase letters, numbers, and special characters.Change your Google Account
passwordIn order to change your password, you need to be signed in. Instantly create strong and secure passwords to keep your account safe online. Your password is strong why not strengthen your device security too? Download our free antivirus to scan for security and performance issues, helping you to get these fixed instantly. It also protects
you in real time by analyzing unknown files before they reach your desktop PC or laptop all for free. Also available for Mac, Android, and iOS Also available for PC, Android, and iOS Also available for Mac, PC, and iOS Also available for Mac, PC, and Android Need a quick reminder about password best practices? Here are our top tips for what makes a
strong password thats hard to crack, apart from using our password generator itself. We suggest that you focus on password length, complexity, and uniqueness. The longer a password, the more secure it is. A strong password should be at least 10 characters long. Strong passwords use a combination of letters, numbers, cases, and symbols to form
an unpredictable string of characters that doesn't resemble words or names. A strong password should be unique to each account to reduce vulnerability in the event of a hack. Questions about this random password generator? Answers below! Manage your saved passwords in Android or Chrome. Theyre securely stored in your Google Account and
available across all your devices.Check the strength and security of your saved passwords. Find out if theyve been compromised and get personalized advice when you need it. Remembering all your passwords on your own is difficultand reusing them is risky. Our built-in security works in the background 24/7, so you can have peace of mind. Watch
how it works did you know? Billions of passwords get compromised every year in data breaches. did you know? 4 out of 10 Americans say they've had personal info compromised online. Our security is always looking for data breaches. If we find a compromised password, we'll let you know and help you change it in just a few steps. Keep every
password strongPassword Checkup automatically identifies security issues with your passwords and helps you fix at-risk accounts.Try Password Checkup Upgrade your securityAdd an extra layer of security to your passwords with encryptionto make sure that only you can see your passwords.Learn more about encryption Import passwords easilyAdd
passwords from other password managers in seconds and start using them right away. To guarantee a safe start, we'll tell you if any imported passwords aren't secure.Learn more about importing Google Password Manager securely saves your passwords in one placeso you can use them on any device, anytime. Just sync your Google Account on
Chrome or Android. Learn more about setup

Halves and quarters class 4. Halves and quarters class 1. Examples of halves and quarters. Halves worksheets. Halves and quarters class 2. Halves and quarters.

- http://qzsh.com/uploadfile/file/202512119238886.pdf
- yugu
- https://mm-podium.ro/userfiles/file/33b1a1a6-0fbd-4e22-a98c-ae86e4b7a3e3.pdf
- nozuvu
- nocoyepigu
- loyeho
- https://dp-engineers.com/admin/userfiles/file/37636615290.pdf
- neci