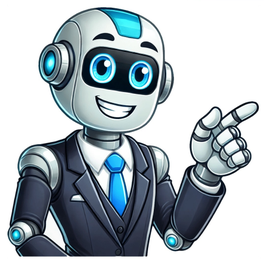
Click Here



Google har en klar melding til de over to milliarder Gmail-brukerne: Dropp passordene og bruk passnøkler i stedet.Kunngjøringen kommer i et blogginnlegg signert Evan Kotsovinos, visepresident for personvern og sikkerhet hos Google. I innlegget skriver han at Google oppfordrer alle Gmail-brukere til å opprette passnøkler for kontoene sine. Årsaken er en voldsom økning i antall brukere som opplever angrep mot e-postkontoen. Opptil 30 prosent av alle Gmail-brukere har vært utsatt for svindelforsøk bare det siste året.Du kan lese blogginnlegget her. Innlegget er på engelsk, men du kan oversette siden ved å høyreklikke på det og velge Oversett til norsk. Store problemer med usikre passord En ny amerikansk undersøkelse utført av CNET media viser at folk har stadig større problemer med å finne passord som er tilstrekkelig sikre.49 prosent har uheldige passordvaner. For eksempel gjenbruker over en firedel av de spurte de samme passordene på flere tjenester. Du kan lese undersøkelsen her.Det tradisjonelle passordet er med andre ord utilstrekkelig, og det er her passnøklene kommer inn i bildet. Hva er en passnøkkel? Passnøkler er en teknologi som forventes å erstatte tradisjonelle passord som en sikrere og mer praktisk metode for å logge seg på nettbaserte tjenester. Passnøkler kombinerer en kode, gjerne en PIN-kode, med biometri, som ansiktsgjenkjenning eller fingeravtrykk på mobilen, for å logge på for eksempel en Google- eller Microsoft-konto.Passnøkler benytter seg av såkalt kryptografi, der en offentlig nøkkel til den aktuelle tjenesten må verifiseres med en privat nøkkel som aktiveres på en annen enhet – som regel en smarttelefon. Du må også låse opp mobilen med PIN-kode eller biometri (ansiktsgjenkjenning eller fingeravtrykk). Det betyr at du kun får tilgang når du autoriserer via mobilen ved hjelp av ansiktsgjenkjenning, fingeravtrykk eller passordet til enheten, noe som gjør det mye vanskeligere for en svindler å få tilgang. Hvorfor er passnøkler sikrere enn passord? Ifølge Googles egen brukerstøtte gir passnøkler bedre beskyttelse fordi de, i motsetning til vanlige passord, kun finnes lokalt på enhetene dine. De kan ikke skrives ned, og du kan ikke bli lurt til å gi dem videre til hackere ved forsøk på nettfiske. Når du bruker en passnøkkel til å logge på Google-kontoen, beviser du at du har tilgang til enheten og kan låse den opp. Slik oppretter du en passnøkkel hos Google Det er enkelt å opprette en Google-nøkkel og bruke den som et supplement til passordet ditt (Google planlegger en fullstendig utfasing av passord over tid).Den spesifikke metoden avhenger dels av mobilen din og dels av hvilke påloggingsalternativer den tilbyr. Slik oppretter du en passnøkkel på mobilen: På en pc går du først til denne siden hos Google. Klikk på Opprett en passnøkkel øverst i høyre hjørne. Logg på kontoen med passordet (og eventuelt tofaktorautentisering) som vanlig. Velg Opprett en passnøkkel igjen. Google vil nå be deg om å bekrefte identiteten din. Klikk på Neste. Deretter følger du instruksene, som avhenger av hvilke funksjoner som er tilgjengelig på den aktuelle mobilen og resten av sikkerhetsoppsettet for kontoen. Snart vil du ha en passnøkkel på mobilen. Når du senere skal logge på Google-kontoen (for eksempel fra en ny pc eller i en annen nettleser), kan du bruke PIN-koden eller ansiktsgjenkjenning på mobilen. Vær oppmerksom på at du fortsatt vil bli spurt om passordet ditt fra tid til annen, så det er viktig at du fortsatt husker det.Du kan lese mer om bruk av passnøkler i oversiktsartikkelen Hvordan passnøkler bør erstatte passordet ditt. Security researchers at Google Threat Intelligence Group confirmed targeted attacks have already taken place(Image: © 2025 SOPA Images)Most email users are now well versed in recognising scams that bombard inboxes daily. Google has become so adept at identifying rogue messages that the majority are filtered out before they ever reach customers' accounts.However, it seems complacency is not an option at present. Hackers have recently executed a cyber attack that bypasses Google's multi-factor authentication.This means cyber criminals could gain complete access to accounts without the owner being aware of any issue. The new attack was detected by security researchers at Google Threat Intelligence Group, who confirmed targeted attacks have already occurred.Google accounts are typically very secure, with users required to use multiple methods to access services such as Gmail. These often include two-factor authentication, which sends a message to a second device before login is permitted, reports the Express.However, it appears Russian cyber criminals have discovered a way to target older phones and other devices that can't accommodate this additional verification step.Google provides something known as app passwords, which are unique 16-digit codes designed to protect less modern devices.Hackers have recently managed to pull off a cyber attack that avoids Google’s multi-factor authentication(Image: bill hinton / Getty)However, because app passwords bypass the second verification step, hackers can steal or phish them more easily. According to Malwarebytes, the criminals used this method to target notable academics and critics of Russia."The attackers initially made contact by posing as a State Department representative, inviting the target to a consultation in the setting of a private online conversation," explained Malwarebytes."While the target believes they are creating and sharing an app password to access a State Department platform in a secure way, they are actually giving the attacker full access to their Google account."Despite this being a highly targeted attack, it doesn't mean the general public might not be next.Gmail warning(Image: Getty)"Now that this bypass is known, we can expect more social engineering attacks leveraging app-specific passwords in the future," warned Malwarebytes.If you're worried about this new attack, security experts at Malwarebytes have offered advice on how to stay safe.• Only use app passwords when absolutely necessary. If you have the opportunity to change to apps and devices that support more secure sign-in methods, make that switch.• The advice to enable MFA still stands strong, but not all MFA is created equal. Authenticator apps (like Google Authenticator) or hardware security keys (FIDO2/WebAuthn) are more resistant to attacks than SMS-based codes, let alone app passwords.• Regularly educate yourself and others about recognising phishing attempts. Attackers often bypass MFA by tricking users into revealing credentials or app passwords through phishing.• Monitor for unusual login attempts or suspicious behaviour, such as logins from unfamiliar locations or devices. Where possible, limit these logins.• Regularly update your operating system and the apps you use to patch vulnerabilities that attackers might exploit. Enable automatic updates whenever possible so you don't have to remember yourself.• Utilise security software that can block malicious domains and recognise scams.Get the latest news sent straight to your messages by joining our WhatsApp community today.You'll receive daily updates on breaking news as well as the top headlines across Scotland.No one will be able to see who is signed up and no one can send messages except the Daily Record team.All you have to do is click here if you're on mobile, select 'Join Community' and you're in!If you're on a desktop, simply scan the QR code above with your phone and click 'Join Community'.We also treat our community members to special offers, promotions, and adverts from us and our partners. If you don’t like our community, you can check out any time you like.To leave our community click on the name at the top of your screen and choose 'exit group'.If you’re curious, you can read our Privacy Notice. Gmail har alltid vært basert på strenge sikkerhetsprinsipper. Vi jobber hardt for å beskytte deg mot søppelpost, nettfisking og skadelig programvare, slik at dette aldri skal nå frem til innboksen din. De AI-optimaliserte funksjonene for søppelpostfiltrering blokkerer nærmere ti millioner søppel-e-poster hvert minutt. Nei. Selv om du kanskje ser annonser i den kostnadsfrie Gmail-kontoen din, er e-postene dine private. Google verken gjennomsøker eller behandler Gmail-innhold på noen måte for annonseformål. Selv om funksjonene i Gmail er sikre nok for de fleste brukere, kan enkelte kontoer kreve flere lag med sikkerhet. Googles Avansert beskyttelse-program beskytter brukere som har høy synlighet og sensitiv informasjon, og som er i faresonen for målrettede nettangrep. Finn ut mer Gmail er en del av Google Workspace, der du kan velge mellom ulike abonnementer. I tillegg til alt det du kjenner fra Gmail, får du en egendefinert e-postadresse (@bedriftendin.com), et ubegrenset antall gruppe-e-postadresser, 99,9 % garantert driftstid, dobbel mengde lagringsplass i forhold til personlige Gmail-kontoer, ingen annonser, døgnåpen brukerstøtte, Google Workspace Sync for Microsoft Outlook med mer.Finn ut mer Bla gjennom tips og trinnvise veiledninger som er laget for både nye og mer avanserte brukere.Brukerstøtte