Varför är Passkeys säkrare än lösenord?

När vi använder lösenord riskerar vi att hackare kommer åt dem genom att gissa sig fram eller använda program som testar miljontals lösenord på kort tid. Med passkeys finns inget lösenord att stjäla, så risken för att bli hackad minskar rejält. En passkey kan inte heller läcka ut på nätet.

Många av oss använder samma lösenord på flera ställen. Detta kan vara riskabelt – om ett ställe hackas, riskerar alla våra konton att bli osäkra. Med passkeys behövs inte längre lösenord, så denna risk försvinner helt.

Mindre risk för nätfiske
Nätfiske är när bedragare försöker lura oss att skriva in våra lösenord på falska webbplatser. Eftersom passkeys kräver att vi godkänner inloggningen på vår egen enhet, kan bedragarna inte komma åt vårt konto, även om vi skulle gå in på en falsk sida.

När du loggar in med en passkey får du en fråga på din enhet, som en mobiltelefon eller dator, om du vill godkänna inloggningen. Du verifierar med ett fingeravtryck, ansiktsigenkänning eller en PIN-kod. Det är snabbt och enkelt, och du slipper krångla med att skriva in ett lösenord!

Alla sajter har inte stöd för detta. Men Amazon, Paypal, X, TikTok och flera andra har det. Det fungerar också med de flesta webbläsare.

Skapa Passkeys

Du kan skapa och spara nycklar som ersätter lösenorden du använder till att logga in i appar som stöds och på webbplatser på iPhone.

Nycklar är säkrare än lösenord eftersom de genereras unikt för varje konto av din egen enhet och är mindre sårbara för nätfiske. Och de fungerar på alla enheter som är inloggade med samma Apple-konto.

Webbplatser och appar kan även skapa nycklar för ditt konto automatiskt så att du kan använda nycklarna nästa gång du loggar in.

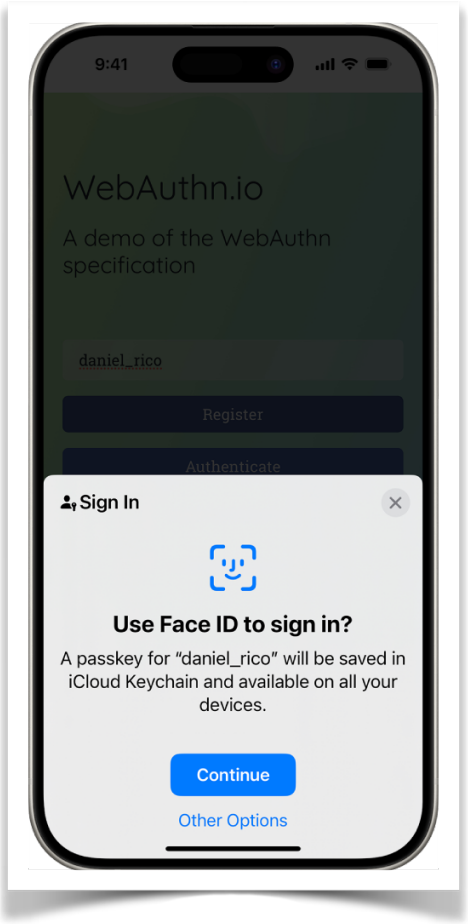
I likhet med lösenord är nycklar krypterade och lagras i iCloud-nyckelring där de inte är synliga för någon (inte ens Apple).

Obs! iCloud-nyckelring och tvåfaktorsautentisering måste vara påslagna för att du ska kunna använda nycklar.

Så slår du på tvåfaktorsautentisering

Öppna ***Inställningar*** > ***[ditt namn]*** > ***Inloggning och säkerhet*** på din iPhone.
Tryck på Slå på tvåfaktorsautentisering och tryck sedan på ***Fortsätt***.
Ange ett betrott telefonnummer (numret du använder till att få verifieringskoder) och tryck sedan på ***Nästa***.
En verifieringskod skickas till ditt betrodda telefonnummer.
Ange verifieringskoden på iPhone.
Tvåfaktorsautentisering slås på för ditt Apple-konto och din iPhone är nu en betrodd enhet.

Skapa och spara en nyckel med iPhone
Du kan skapa och spara nycklar för appar och webbplatser som stöder dem. Anvisningarna för att skapa och spara en nyckel kan dock variera beroende på app, webbplats eller webbläsare, men de liknar vanligtvis stegen nedan.



Navigera till inloggningsskärmen för en webbplats eller app som stöds på iPhone/iPad eller Mac och gör något av följande:
Om du skapar ett nytt konto: Tryck på knappen eller länken för att skapa ett nytt konto och följ sedan anvisningarna på skärmen.

Om du redan har ett konto: Logga in med ditt kontonamn och lösenord och öppna sedan skärmen för kontoinställningar eller kontohantering.

När du ser alternativet för att spara en nyckel för kontot trycker du på Fortsätt. Nyckeln sparas.

Obs! Om du inte ser ett nyckelalternativ innebär det att webbplatsen eller appen för närvarande saknar stöd för nycklar.

Nycklarna som du skapar lagras på i appen Lösenord. Du kan ha en nyckel och ett lösenord för samma webbplats eller app och hitta båda under samma konto i appen Lösenord.

Använd en nyckel som har sparats på iPhone till att logga in på en annan enhet

Om du använder en enhet som inte är associerad med ditt Apple-konto (t.ex. en dator på ett bibliotek, ett internetkafé eller hos en vän), och du har din iPhone med dig, kan du logga in i appar och på webbplatser på den enheten med nycklarna du har skapat för dem. Anvisningarna för att logga in med en nyckel på en annan enhet kan variera beroende på app, webbplats eller webbläsare, men de liknar vanligtvis stegen nedan.

Öppna webbplatsen eller appen på den andra enheten och ange ditt användarnamn i kontonamnsfältet på inloggningsskärmen.

Välj ***Andra alternativ***, ***Nyckel från enhet i närheten*** eller liknande och följ sedan anvisningarna på skärmen för att visa en QR-kod på skärmen. Använd sedan iPhone-kameran till att skanna QR-koden. Nyckeln som är sparad i iCloud-nyckelring slutför inloggningen automatiskt.

Webbplatser som har stöd för Passkeys
Amazon.se
Paypal.com
Dropbox
Facebook

Google
Yahoo
Justwatch

Passkeys fungerar bara på IOS 16 eller senare. För Mac gäller Mac OS Ventura (Mac OS13) eller senare.

Allmänt säkerhetstänkande
Smishing är en form av nätfiske som använder SMS för att lura mottagare att avslöja känslig information eller klicka på skadliga länkar. Namnet kommer från en kombination av "SMS" och "phishing." Precis som i andra phishing-attacker, utger sig angriparen ofta för att vara en betrodd källa, som en bank, ett företag eller till och med en vän. Något som förmodligen kommer att öka den närmaste månaden då vi närmar oss black friday och jul.

Hur fungerar smishing?

1. Bedrägliga meddelanden: Ett typiskt smishing-meddelande kan se ut att komma från en betrodd källa och innehålla ett meddelande som väcker stress eller nyfikenhet, till exempel "Ditt konto har blivit låst" eller "Du har vunnit ett pris."
2. Falska länkar eller uppmaningar: Meddelandet innehåller ofta en länk till en falsk webbplats eller uppmanar mottagaren att svara med känslig information. Länken kan leda till en sida som ser legitim ut men är avsedd att stjäla information eller sprida skadlig programvara.
3. Social ingenjörskonst: Smishing utnyttjar människors förtroende och rädsla för att få dem att agera snabbt, utan att noggrant undersöka meddelandet.

Exempel på smishing-attacker

• Ett SMS som påstår sig vara från din bank och ber dig att klicka på en länk för att "säkerställa ditt konto".
• Ett meddelande från ett "leveransföretag" som säger att ditt paket är på väg och ber dig klicka på en länk för att spåra det.
• Ett SMS som påstår sig komma från en vän eller familjemedlem som lånat en kompis telefon med en uppmaning om att skicka tillbaka pengar eller hjälp med något akut.

Hur man skyddar sig mot smishing:

1. Klicka aldrig på okända länkar i SMS, särskilt om de kommer oväntat eller verkar misstänksamma.
2. Kontakta företaget direkt om du får ett meddelande från en bank eller ett företag. Använd den officiella webbplatsen eller appen för att kontrollera meddelandets äkthet.
Öppna aldrig BankID!
3. Dela inte personlig information som bankuppgifter eller lösenord via SMS, oavsett hur legitimt meddelandet ser ut.
4. Apples egna mail-program brukar sortera ut misstänkta spam

Smishing är en ökande hottyp, så det är viktigt att vara vaksam och ifrågasätta alla oväntade meddelanden som ber om information eller åtgärder.

Phishing

Phishing är en form av bedrägeri där angripare försöker lura människor att avslöja känslig information, som lösenord, kreditkortsnummer eller personliga uppgifter. Namnet kommer från engelskans ord för fiske – angripare "fiskar" efter information genom att använda olika metoder för att vilseleda och utnyttja mottagarnas förtroende.

Hur fungerar phishing?
1. Phishing-attacker kommer ofta i form av e-postmeddelanden som ser ut att komma från en pålitlig källa, som en bank, ett företag eller en myndighet. De innehåller vanligtvis en länk till en falsk webbplats som liknar en riktig, där användaren ombeds att ange sina inloggningsuppgifter eller annan information.

2. Social manipulering: Angripare använder psykologiska metoder för att skapa en känsla av brådska, rädsla eller nyfikenhet. Ett phishing-meddelande kan exempelvis säga "Ditt konto har blivit låst" eller "Du måste uppdatera din betalningsinformation omedelbart."

3. Manipulerade länkar och bilagor: Meddelanden kan innehålla länkar som ser legitima ut men leder till skadliga webbplatser, eller bilagor som innehåller skadlig kod. När mottagaren klickar på dessa kan deras dator infekteras, eller så kan deras data stjälas.

Exempel på phishing

• Bankphishing: Ett e-postmeddelande som verkar komma från din bank och ber dig logga in för att "verifiera ditt konto."
• PayPal eller e-handelsbedrägeri: Ett falskt meddelande från en betaltjänst eller ett företag som ber dig bekräfta en transaktion som du inte har gjort.
• Falska säkerhetsvarningar: Ett e-postmeddelande från en "säkerhetsavdelning" som ber dig ändra ditt lösenord på grund av ett "säkerhetsbrott."

Hur skyddar man sig mot phishing?
1. Kontrollera alltid avsändaren: Var noga med e-postadresser och webbplatsadresser, särskilt om meddelandet är oväntat eller verkar misstänkt. Små förändringar, som ett extra tecken i e-postadressen, kan vara en varningssignal.
2. Klicka inte på okända länkar eller bilagor: Om ett meddelande innehåller länkar, hovra över dem för att se var de leder innan du klickar. Ladda endast ner bilagor från kända och betrodda avsändare.
3. Kontakta företaget direkt: Om du får ett meddelande från en bank eller ett företag som ber om känslig information, kontakta dem via officiella kanaler för att bekräfta meddelandets äkthet.
4. Öppna aldrig BankID! Om ngn säger att de ringer från din bank så ljuger de med största sannolikhet. Be om att få motringa. Knappa in bankens hemsida manuellt i din webbläsare och ring numret som står där. Klicka inte på bifogade länkar eller telefonnummer.

Phishing är en av de vanligaste cyberbedrägerierna, så det är viktigt att vara vaksam och ifrågasätta alla meddelanden som ber om personlig eller finansiell information.

Social manipulation-attacker
Social engineering innebär att angripare manipulerar människor att avslöja känslig information. Förutom phishing och smishing ingår även "vishing" (voice phishing), där angriparen ringer offret och utger sig för att vara någon pålitlig, till exempel kundtjänst från banken, för att få tillgång till kontouppgifter. Oftast är det brådskande. De kan till exempel påstå att ditt konto blivit kapat och du måste åtgärda detta omedelbart.

Öppna aldrig BankID! Om ngn säger att de ringer från din bank. Be om att få motringa. Knappa in bankens hemsida manuellt och ring numret som står där. Klicka inte på bifogade länkar eller telefonnummer.

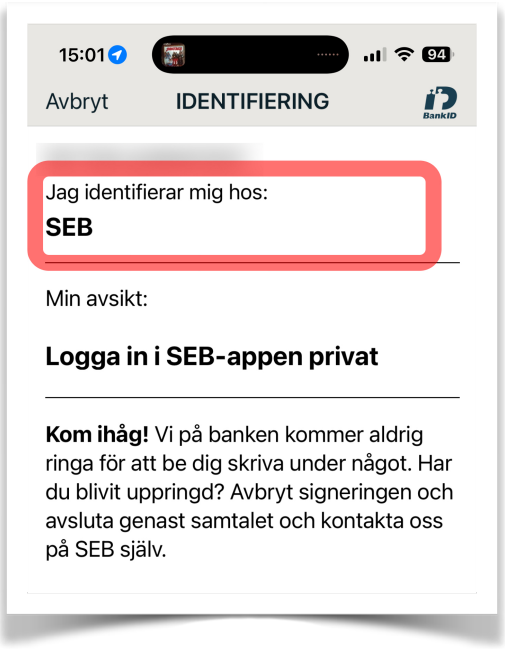
Rent generellt gäller detta:
Om något låter för bra för att vara sant är det förmodligen så. Ett erbjudande som är mycket billigare på nätet än IRL är förmodligen en bluff.

Din bank skulle aldrig ringa dig för att varna om att ”ditt konto håller på att bli hackat”. Om banken upptäckter ett obehörigt dataintrång i sina system är du den sista personen de kommer att ringa.

Överlista försök till social manipulation genom att ställa motfrågor. Det förekommer nu att människor får SMS från ett okänt nummer, men den som skickar sms:et påstår sig vara barn eller barnbarn som har ”tappat” sin telefon och nu använder sin kompis telefon och behöver hjälp med Swish eller BankID.

Kontrollera varje gång du använder BankID att du legitimerar dig mot rätt bank/tjänst/person.

Om du är osäker. Ta ett djupt andetag innan du öppnar ditt BankID och bjuder in skurken till ditt bankkonto. Tänk efter *innan* du gör något.



Kontroller att du verkligen identifierar dig mot rätt företag/person.