Kensington®

Glem dit password

Det sikreste log-in er din fingerspids

Dine medarbejdere er den største trussel mod din datasikkerhed

Antallet af databrud stiger støt. Der vurderes at have været 8,5 milliarder databrud i 2019[1], mere end 70 % mere end 2018.[2]

Hacking (brug af angrebsværktøjer til at få adgang til beskyttede oplysninger) og phishing (udgive sig for en pålidelig kilde, så fortrolige data udleveres) er de mest almindelige cyberangreb, der bruges til at forårsage databrud. **80 % af hacking-relaterede brud forårsages af kompromitterede, svage og genbrugte passwords.**[3]

"Sikre" adgangskoder – brug af store bogstaver, små bogstaver, tal og symboler – er lette at glemme. Når man påtænker, at en gennemsnitlig bruger har 191 passwords[4], bliver de en reel udfordring at håndtere.

I stedet for at stole udelukkende på brugernavne og adgangskoder giver multifaktorgodkendelse (MFA) et yderligere sikkerhedslag. **Når der kræves en yderligere faktor for at give adgang, er biometrisk godkendelse det sikreste niveau af MFA.**

MFA kan implementeres problemfrit i brugerarbejdsgange, hvor Windows Hello understøtter biometrisk logon og passwordfri adgang til onlinetjenester. FIDO Alliance har udarbejdet standarder til maksimering af kompatibiliteten for enheder.

Kensington VeriMark™ USB-fingeraftryksnøgle

- ☑ Biometrisk logon
- ☑ Understøtter MFA
- ☑ Windows Hello
- ☑ FIDO U2F-certificeret

Kensington®

Det er på tide at glemme din adgangskode

Enkeltfaktorgodkendelse – med andre ord et password, der ikke kræver yderligere godkendelse – ses af hackere som den mest ubesværede vej. Når det lykkes med en phishing-kampagne eller et genafspilningsangreb at høste et password, giver det mulighed for at stjæle endnu flere oplysninger, når adgangen til enheden er kompromitteret.

Passwords, selv stærke, er ikke længere nok til at beskytte følsomme konti og aktiver mod hacking- og phishing-angreb.

Der er en nær forbindelse mellem sikkerhed, der kun er baseret på password, og databrud, fordi de begge viderefører en ondsindet cyklus af dyr informationstyveri.

Dine passwords er ikke sikre nok

Uden yderligere sikkerhedsmetoder er passwords skrøbelige mod rutinemæssigt tyveri og opsnapning. **Tofaktorgodkendelse** (eller flerfaktorgodkendelse) bør være del af ethvert moderne sæt af godkendelsesprotokoller.

Ved at kræve endnu en oplysning (eller faktor) ud over et password eller to unikke oplysninger uden password i det hele taget undgår 2FA/MFA de kendte kompleksiteter og mangler ved passwordbaserede logon.

Unikke biometriske legitimationsoplysninger, f.eks. fingeraftryk, er langt bedre end traditionelle sms'er og sikkerhedsspørgsmål, som kan opsnappes, uden at brugeren ved det. Godkendelsesteknologi har udviklet sig med introduktionen af biometriske løsninger, f.eks. Microsofts Windows Hello-logon[5], som er kompatible med **Kensingtons VeriMark™-fingeraftryksnøgle.**

Hvorfor 2FA og MFA?

Den grundlæggende fejl i enkeltfaktorbaseret passwordsikkerhed er, at hvis en uautoriseret part har det rigtige logon, har denne adgang til den passwordbeskyttede konto. **Det er ligegyldigt, om passwordet blev opnået gennem tyveri, et systematisk ordbogsangreb eller heldigt gæt: Den resulterende risiko er den samme.**

To- og multifaktorgodkendelse ændrer godkendelsesmodellen til det bedre på to afgørende måder:

- Der kræves verificering af endnu en legitimationsoplysning efter vellykket indtastning af password.
- Logon tillades udelukkende gennem en mere sikker mekanisme uden password.

Under alle omstændigheder vil godkendelsesløsningen forsøge at verificere en brugers identitet ved at kræve noget, som **brugeren ved, har eller kan identificeres med.** Mulighederne går fra et engangspassword, der sendes med sms eller genereres i en godkendelsesapp, til noget betydeligt stærkere såsom en hardware- eller fingeraftryksnøgle. De to sidstnævnte giver større sikkerhed, fordi de ikke er skrøbelige over for opsnapning eller phishing.

Fordelene ved biometri til 2FA, MFA og logon uden password

Biometri giver en unik kombination af praktisk brug og sikkerhed, fordi det er:

- **Let at scanne, verificere og forbinde med en specifik enhed.**
- **Baseret på legitimationsoplysninger, der er svære at dublere eller stjæle.**
- **Gemmes eller overføres gennem specialiseret hardware for at forhindre fjernadgang eller tyveri.**

Biometrisk godkendelse kan give mere end bare en bedre logonoplevelse for slutbrugere.

Biometri muliggør logon uden password, som reducerer IT-hjælpens arbejdsbyrde til nulstilling af passwords. Hver passwordnulstilling anslås at koste mere end 445 kr.[6] - og mere end 40 % af brugere kræver mere end 50 nulstillinger om året.[7]

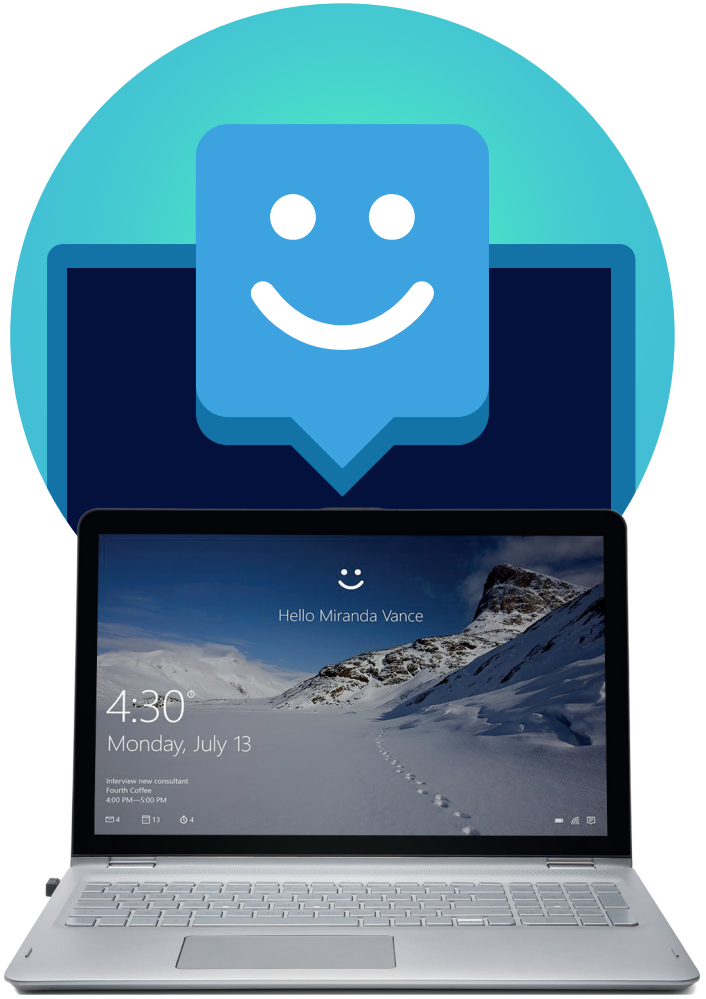
I en organisation med 1000 brugere betyder det op til 8,9 million kr. om året i mistet tid og produktivitet.

Windows Hello understøtter øjeblikkeligt biometrisk logon

Windows Hello, der er en standardfunktion i Windows 10, understøtter øjeblikkelig biometrisk logon. Disse biometriske muligheder omfatter ansigtsgenkendelse, irisscanning og fingeraftryksaflæsning, **det sidstnævnte via FIDO U2F-certificeret hardware såsom Kensington VeriMark™-fingeraftryksnøgle.**

Windows Hello eliminerer ubelejligheden ved at oprette og huske komplekse adgangskoder. Hvad vigtigere er, undgår det de almindelige smuthuller i passwordbaseret sikkerhed, f.eks. eksponering af legitimationsoplysninger via phishing.

Logonoplevelsen i Windows Hello er total ligefrem. Vellykket biometrisk godkendelse låser adgangen til en understøttet Windows-enhed op.



Hvad er FIDO?

Fast IDentity Online (FIDO) Alliance blev etableret for at sætte standarder for både 2FA/MFA og godkendelse uden password.

FIDO Universal Second Factor (U2F) er en åben standard, der definerer specifikationer for 2FA gennem brug af en robust og manipulationssikret anden faktor uden brug af password. Fordi FIDO U2F er standardiseret, er den generelt kompatibel med populære onlinetjenester, herunder Gmail, Facebook, GitHub, Dropbox og mange andre.

Biometriske fingeraftryks- og hardwarenøgler, der bruger USB-, NFC- eller Bluetooth-teknologier, er de typiske yderligere faktorer for tjenester, der anvender U2F.

VeriMark™ – den første fingeraftrykssikkerhedsnøgle fra Kensington, som sikrer stærk, strømlinet 2FA

VeriMark™ fungerer sammen med både Windows Hello- og FIDO U2F-godkendelse for at give en sikker og problemfri måde at logge på Windows 7, 8.1 og Windows 10 samt muliggøre brugen af 2FA på vigtige konti.

VeriMark™-fingeraftryksnøglen byder på den bedste biometriske ydeevne i sin klasse i en praktisk, kompakt og standardoverholdende pakke.

Falske afvisningsrater (3 %) og falske acceptrater (0,002 %), som overstiger branchestandarder ved at udnytte TLS1.2/AES256-kryptering og teknologi til forfalskningsbeskyttelse (ASP).

VeriMark™ er den perfekte løsning til personer, der kræver biometrisk godkendelse, der fungerer sammen med aktuelle eller ældre Windows-operativsystemer, og samtidigt understøtter U2F-godkendelse til skybaserede service- og softwareudbydere, f.eks. Facebook, Google, GitHub, Dropbox og flere.

Kensington VeriMark™-fingeraftryksnøgle

- **Avanceret fingeraftrykteknologi** kombinerer suveræn biometriske ydeevne og 360° læsbarhed med forfalskningsbeskyttelse og overstiger samtidigt branchestandarder for falsk afvisningsrate (3 %) og falsk acceptrate (0,002 %).
- **Universel integration** giver skalerbar, out-of-the-box-adgang til Windows-computere og -platforme, herunder biometrisk logon til Windows Hello™.
- **FIDO U2F-certificeret** for at sikre problemfri kompatibilitet og opfylde kravene til tofaktorlogon med sikkerhedsnøgle til skybaserede tjeneste- og softwareudbydere, herunder Google, Dropbox, GitHub og Facebook.
- **Kompakt design** betyder let fastgørelse til en almindelig nøglering, som let kan bæres rundt.

Varenr. K67977WW

Flere oplysninger, samples eller aftalepriser:

 www.kensington.com/forget-your-password

 contact@kensington.com

Kilder

1. Risk Based Security's Q3 2019 Data Breach QuickView Report
2. darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875
3. Verizon 2019 Data Breach Investigations Report
4. securitymagazine.com/articles/88475-average-business-user-has-191-passwords
5. symantec.com/content/en/uk/enterprise/other_resources/b-is-your-data-safe-security-non-compliance-infographic-21330416-UK.pdf
6. infosecurity-magazine.com/opinions/how-much-passwords-cost
7. plan-net.co.uk/blog/password-reset-processes