OUCH! | September 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

Password Managere

Oversigt

Et af de vigtigste skridt du kan tage for at beskytte dig selv online er at bruge et unikt og stærkt kodeord til hver enkelt af dine konti og apps. Desværre er det højst sandsynligt umuligt for dig at huske forskellig adgangskode til hver af dine forskellige konti. Derfor genbruger mange mennesker de samme adgangskoder. Desværre er genbrug af samme adgangskode til forskellige konti farligt, fordi når en person kompromitterer dit kodeord, kan han få adgang til alle dine andre konti, der brugte samme adgangskode. En simpel løsning er at bruge en password manager. Dette er et program, der på en sikker måde gemmer alle dine adgangskoder, hvilket gør det nemt at få en unik adgangskode til hver konto. En password manager gør det simpelt, fordi i stedet for at skulle huske alle dine adgangskoder, behøver du kun at huske hovedadgangskoden til din password manager.

Gæsteredaktør

Chris Christianson er en informationssikkerhedskonsulent med base i Californien med 20 års erfaring og mange tekniske certificeringer. Han har talt ved en række konferencer og har bidraget til mange artikler. Chris kan nås på **@cchristianson** og **https://ismellpackets.com**.

Sådan fungerer en password manager

Password managere gemmer alle dine adgangskoder i en database. Password manageren krypterer indholdet og beskytter den med et hovedadgangskode, som kun du ved. Når du skal hente dine adgangskoder, for eksempel for at logge ind på din online bank eller e-mail, skal du blot skrive din hovedadgangskode til din password manager for at låse op for kodeordene. I mange tilfælde vil password manageren automatisk hente dit kodeord og sikkert logge ind for dig. Dette gør det nemt at have hundredvis af unikke, stærke adgangskoder, da du ikke behøver at huske dem.

Nogle password managere gemmer din database på din computer eller din mobilenhed, mens andre gemmer det i skyen. Derudover har de fleste password managere evnen til automatisk at synkronisere din database på tværs af flere enheder, som du har godkendt. På denne måde, vil du, når du opdaterer et kodeord på din bærbare computer, få synkroniseret disse ændringer til alle dine andre enheder. Uanset hvor databasen er gemt, skal du installere password manager programmet på de systemer eller enhed hvor du ønsker at bruge det.

© SANS Institute 2017

Password Managere

Når du første gang opretter en password manager, skal du manuelt indtaste eller importere dine login og adgangskoder. Derefter kan password manageren opdage, når du forsøger at registrere dig på en ny online-konto eller opdaterer adgangskoden til en eksisterende konto, og automatisk opdatere database. Dette er muligt, fordi de fleste password managere arbejder sammen med din webbrowser. Denne integration giver dem også mulighed for automatisk at logge dig ind på hjemmesider.

Password managere er en nem måde til sikkert at gemme og bruge forskellige adgangskoder.

Det er afgørende, at den hovedadgangskode, du bruger til at beskytte din password managerens indhold, er stærk og meget svær for andre at gætte. Faktisk anbefaler vi, at du som din hovedadgangskode benytter dig af en passphrase, en af de stærkeste typer af adgangskoder, der er mulige. Hvis din password manager understøtter to-trins verifikation, skal du bruge det til din hovedadgangskode. Endelig skal du huske din hovedadgangskode. Hvis du glemmer den, vil du ikke kunne få adgang til nogle af dine andre adgangskoder.

Valg af password manager

Der er mange password managere at vælge imellem. I afsnittet ”Hvis du vil vide mere” giver vi et link til anmeldelser af forskellige password managere. Når du forsøger at finde den der er bedst for dig, skal du huske følgende:

- Din password manager skal være enkel for dig at bruge. Hvis du finder løsningen for kompleks, skal du finde en anden, der passer bedre til din stil og ekspertise.
- Din password manager skal arbejde på alle de enheder, hvor du bruger adgangskoder. Det skal også være nemt at holde dine adgangskoder synkroniseret på tværs af alle dine enheder.
- Brug kun velkendte og betroede password managere. Vær forsigtig med produkter, der ikke har eksisteret i lang tid eller har ringe eller ingen anmeldelser. IT-kriminelle kan oprette falske password managere for at stjæle dine oplysninger. Vær også mistænksom hvis leverandøren reklamerer med at de selv har udviklet deres krypteringsløsning.
- Undgå enhver password manager, der hævder at kunne genskabe din hovedadgangskode til dig. Det betyder, at de kender din hovedadgangskode, hvilket udsætter dig for en stor risiko.

© SANS Institute 2017

Password Managere

- Sørg for, uanset hvilken løsning du vælger, at sælgeren fortsætter med aktivt at opdatere og patche password manageren. Sørg for, at du altid bruger den nyeste version.
- En password manager skal indeholde evnen til automatisk at generere stærke adgangskoder og vise dig styrken af de adgangskoder, du har valgt.
- En password manager skal give dig mulighed for at lagre andre følsomme data, f.eks. svarene på dine hemmelige sikkerhedsspørgsmål, kreditkort eller hyppige flyvenumre.

Password managere er en fantastisk måde til sikkert at gemme alle dine adgangskoder og andre følsomme data. Men da de beskytter sådanne vigtige oplysninger, skal du sørge for at bruge en unik og stærk hovedadgangskode, der ikke kun er svær for en hacker at gætte, men som også er nem for dig at huske.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Tidligere udgivelser

Top Password Managers of 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Passphrases (oversat til dansk):	https://securingthehuman.sans.org/ouch/2017#april2017
Totrinsbekræftelse:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS Security Tip of the Day:	https://www.sans.org/tip-of-the-day

Licensinformation

OUCH! er udgivet af SANS Securing The Human og distribueres under Creative Commons BY-NC-ND 3.0 licensen. Du er velkommen til at videregive dette nyhedsbrev eller bruge det i dit eget arbejde med IT-sikkerhed så længe du ikke ændrer i nyhedsbrevet. Hvis du har spørgsmål til oversættelsen eller andet er du velkommen til at kontakte ouch@securingthehuman.org.

Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity