OUCH! | April 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Passphrases eller kode-sætninger**
- **Sikker brug af passphrases**
- **Hvis du vil vide mere**

Passphrases

Baggrund

Adgangskoder er noget, du bruger næsten hver dag, for at få adgang til din e-mail, netbank, købe varer eller få adgang til din smartphone. Men adgangskoder er også et af dine svageste punkter; hvis nogen lærer eller gætter dit password, kan de få adgang til dine konti, som om de er dig. Dette vil give dem mulighed for at overføre penge, læse dine e-mails eller stjæle din identitet. Derfor er stærke passwords afgørende for at beskytte dig selv. Imidlertid har adgangskoder typisk været svære at huske og svære at skrive. I dette nyhedsbrev vil du lære, hvordan du opretter stærke adgangskoder, der er nemme for dig at huske og enkle at skrive - disse kaldes ”passphrases” eller ”kode-sætninger”.

Gæsteredaktør

Min-Ngoc Nguyen (udtales Me-Nop Wynn) er en certificeret SANS instruktør og ”CEO / Principal Consultant” ved ”Secured IT Solutions”. Hun har ekspertise og top certificeringer og mere end 14 års udvikling, forbedring af og administration af IT-sikkerhedsprogrammer for forskellige brancher og sektorer. Twitter: **@MenopN** LinkedIn: My-Ngoc “Menop” Nguyen.

Passphrases eller kode-sætninger

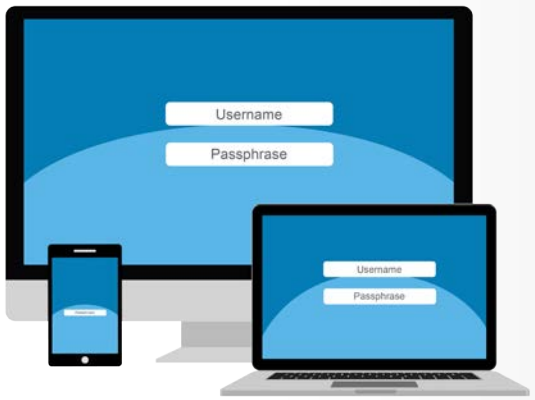
Den udfordring, vi alle står overfor, er at IT-kriminelle har udviklet avancerede og effektive metoder til at gætte adgangskoder – Kaldet ”brute force”. Det betyder, at IT-kriminelle kan kompromittere dine passwords, hvis de er svage eller lette at gætte. Et vigtigt skridt til at beskytte dig selv, er at bruge stærke adgangskoder. Dette har man typisk gjort ved at skabe komplekse passwords, men disse kan være svært at huske, forvirrende og vanskelige at skrive. I stedet anbefaler vi, at du bruger passphrases eller kode-sætninger. En passphrase eller en kode-sætning er en række tilfældige ord eller en sætning. Jo flere tegn dit kodeord har, jo stærkere det er. Fordelen er, at disse er meget lettere at huske og skrive, men de er stadig svære for IT-kriminelle at hacke. Her er to forskellige eksempler.

Udhold-Nemt-Fængsel
Tid til te klokken 01:23

Det, der gør disse kodeord så stærke, er ikke kun, at de er lange, men at de bruger store bogstaver og symboler (husk, mellemrum og tegnsætning er symboler). Samtidig er disse passphrases også lette at huske og skrive. Du kan gøre dit kodeord endnu stærkere, hvis du ønsker. Det gør du ved at erstatte bogstaver med tal eller symboler,

Passphrases

såsom udskiftning af bogstavet ”a” symbolet med “@” eller bogstavet “o” med tallet ”0”. Hvis et websted eller et program har en begrænsning på antallet af tegn, du kan bruge i en adgangskode, bør du bruge det maksimale antal tilladte tegn.



Passphares er en simple måde at lave og huske stærke kodeord.

Sikker brug af Passphrases

Du skal være forsigtige med, hvordan du bruger dine passphrases. Brug af en adgangskode vil ikke hjælpe, hvis de IT-kriminelle nemt kan stjæle eller kopiere den.

1. Brug forskellige passphrases til alle dine konti eller enheder. Eksempelvis må du aldrig bruge den samme adgangskode til arbejde eller bankkonto, som du bruger til dine personlige konti, såsom Facebook, YouTube eller Twitter. Hvis du bruger forskellige passphrases og den ene konto bliver hacket, er dine andre konti stadig sikre. Hvis du har for mange passphrases til, at du kan huske dem (hvilket er meget almindeligt), bør du overveje at bruge en ”password manager”. Dette er et særligt program, der på en sikker måde gemmer alle dine passphrases. Hvis du bruger en ”password manager”, er de eneste passphrases du skal huske, dem til computeren eller enheden og til ”password manager”.
2. Del aldrig en adgangskode eller din strategi for at skabe adgangskoder med andre, herunder kollegaer eller overordnede. Husk, et kodeord er en hemmelighed; hvis en anden kender dit kodeord er det ikke længere sikkert. Hvis du ved et uheld deler en adgangskode med en anden, eller tror dit kodeord kan være blevet kompromitteret eller stjålet, skal du straks ændre det. Den eneste undtagelse er, hvis du ønsker at dele dine vigtigste personlige passphrases med et højt betroet familiemedlem i tilfælde af en nødsituation. En fremgangsmåde er at skrive dine vigtigste personlige passphrases ned (sørg for at de ikke er arbejdsrelaterede), gemme dem på et sikkert sted, og dele denne placering med et meget betroet familiemedlem. Hvis der sker noget med dig, og du har brug for hjælp, kan dine kære få adgang til dine vigtige konti.
3. Brug ikke offentlige computere, så som dem på hoteller eller internetcaféer til at logge ind på dine konti. Da alle kan bruge disse computere, kan de være inficeret og indfange alle dine tastetryk. Du bør kun logge ind på din konto på computere eller mobile enheder du har tillid til.
4. Vær forsigtig med hjemmesider, der kræver, at du besvare personlige spørgsmål. Disse spørgsmål bruges, hvis du glemmer dit passphrase og har brug for at nulstille den. Problemet er, at svarene på disse spørgsmål ofte kan findes på internettet, eller endda på din Facebook-side. Sørg for, at hvis du svarer med personlige oplysninger, så bruger

Passphrases

du kun oplysninger, der ikke er offentligt tilgængelige eller fiktive oplysninger, som du selv har fundet på. Kan ikke huske alle svar på dine sikkerhedsspørgsmål? Vælg et tema eksempelvis en filmkarakter som du baserer dine svar på. En anden mulighed er igen at bruge en "password manager", de fleste af dem giver dig også mulighed for at opbevare disse supplerende oplysninger på en sikker måde.

5. Mange online konti tilbyder noget, der hedder to-faktor-autentificering, også kendt som to-trins bekræftelse. Her har du brug for mere end bare et kodeord for at logge ind, eksempelvis kan det være en adgangskode der sendes til din smartphone. Denne mulighed er meget mere sikker end blot en adgangskode i sig selv. Når det er muligt, skal du altid aktivere og bruge disse stærkere metoder til godkendelse.
6. Mobile enheder kræver ofte en PIN-kode for at beskytte adgangen til dem. Husk en PIN er intet mere end en adgangskode. Jo længere din PIN-kode er, desto sikrere er det. Mange mobile enheder giver dig mulighed for at ændre din PIN-kode til et egentligt kodeord eller bruge en biometrisk såsom dit fingeraftryk.
7. Hvis du ikke længere bruger en konto, skal du sørge for at lukke, slette eller deaktivere den.

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

Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Two Step Verification(oversat til dansk):	https://securingthehuman.sans.org/ouch/2015#september2015
Lock Down Your Login:	https://lockdownyourlogin.com
SANS SEC301 - Five day course on cyber security basics:	https://sans.org/sec575

Licensinformation

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