OUCH! | Juli 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Sikring af dig selv**
- **Sikring af dit system**
- **Til forældre eller værger**

Spil sikkert på nettet

Oversigt

Online spil er en fantastisk måde at have det sjovt på, men der er også nogle unikke risici. I dette nyhedsbrev fortæller vi hvad du og din familie kan gøre for at beskytte jer når du spiller online.

Gæsteredaktør

Steve Armstrong er grundlægger af "Logically Secure". Han er certificeret SANS instruktør og arkitekten bag CyberCPR en "Incident Management Platform". Han er aktiv på Twitter som **@Nebulator** og arbejder med mange store spilvirksomheder i verden. Han opfylder både sine barndomsdrømme og sine professionelle drømme!

Sikring af dig selv

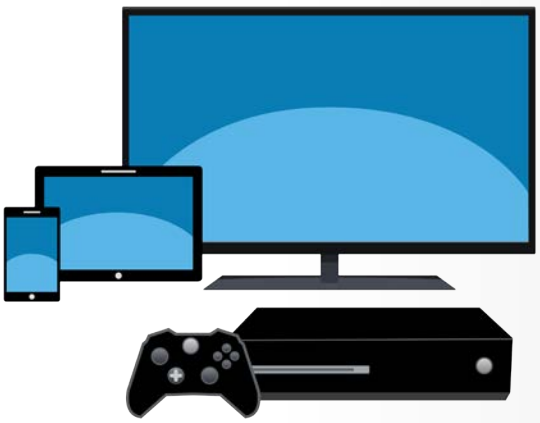
Det, der gør online spil så sjovt er, at du kan spille og kommunikere med andre fra hele verden. Ofte kender du måske ikke engang de mennesker, du spiller med. Mens det store flertal af mennesker online er ude på at have det sjovt ligesom dig, er der dem, der vil forårsage skade. Her er nogle råd, du kan følge for at være sikker.

- Vær forsigtig med eventuelle meddelelser, der beder dig om at foretage en handling, såsom at klikke på et link eller downloade en fil. Ligesom e-mail phishing-angreb vil onde fyre forsøge at narre eller snyde dig i onlinespil til at gøre noget, der kan inficere din computer eller stjæle din identitet. Hvis en meddelelse virker underlig eller for god til at være sandt, så skal du være mistænksom overfor om det kan være et angreb.
- Mange onlinespil har deres egne finansielle markeder, hvor du kan handle, bytte eller endda købe virtuelle varer. Ligesom i den virkelige verden er der svindlere i disse systemer, som vil forsøge at narre dig og stjæle dine penge eller virtuel valuta, du har samlet. Handel kun med folk, der har et godt ry.
- Brug en stærk adgangskode til alle spilkonti. På denne måde kan angribere ikke bare gætte dine adgangskoder og overtage dine konti. Hvis dit spil tilbyder to-trins verifikation, skal du bruge den. Desuden skal alle dine online-konti have forskellige adgangskoder. På den måde er dine andre konti sikret selvom et spil bliver kompromitteret. Kan du ikke huske alle dine adgangskoder? Overvej en adgangskode manager.

Sikring af dit system

IT-kriminelle kan forsøge at hacke eller overtage den computer, du spiller på, du skal derfor tage følgende skridt til at beskytte den.

Spil sikkert på nettet



Nøglen til sikker gaming online er at bruge stærke adgangskoder, sikre din computer og bruge sund fornuft, når du modtager meddelelser eller anmodninger.

- Du skal sikre din computer ved altid at køre den nyeste version af operativsystemet og spilsoftwaren. Gammelt og forældet software har kendte sårbarheder, som angriberne kan udnytte og bruge til at hacke din computer. Ved at holde din computer og spil applikationer opdateret fjerner du de fleste af de kendte sårbarheder.
- Du skal bruge anti-virus software og sørge for, at den opdateres og kontrollerer alle filer, du kører i realtid.
- Du skal kun downloade spilsoftware fra betroede websteder. Ofte vil IT-kriminelle skabe en falsk eller inficeret version af et spil og distribuere det fra deres egen server.
- Gaming add-on-pakker, som ofte udvikles af fællesskabet, bruges ofte til at tilføje nye funktioner. IT-kriminelle inficerer undertiden disse spilpakker med malware. Ligesom når du downloader spil, skal du også sørge for at downloade tilføjelsesprogrammerne fra pålidelige steder. Desuden skal du ikke bruge det, hvis en tilføjelse kræver, at du deaktiverer din antivirus eller ændrer dine sikkerhedsindstillinger.
- Undergrundsmarkeder er dukket op for at understøtte snydaktivitet. Udover at være uetiske, er mange snydprogrammer selv malware, der vil inficere din computer. Installer eller brug aldrig nogen form for snydesoftware eller hjemmesider.
- Du skal undersøge webstedet for den online gaming software, du bruger. Mange gaming sites har et afsnit om, hvordan du sikrer dig selv og dit system.
- Alle disse råd gælder også hvis du spiller online spil på dine mobile enheder. IT-kriminelle begynder også at målrette deres angreb mod mobile enheder.

Til forældre eller værger

Børn kræver ekstra beskyttelse og uddannelse, når de spiller online. Uddannelse og en åben dialog med dine børn er et af de mest effektive skridt, du kan tage for at beskytte dem. Et af vores foretrukne tricks for at få børnene til at tale er at bede dem om at vise dig, hvordan deres spil fungerer, få dem til at vise dig deres online verden og vise dig, hvordan et typisk spil ser ud. Måske endda spille spillet med dem. Desuden skal de beskrive de forskellige personer, de møder online. Ofte kan online gaming være en stor del af dit barns sociale liv. Ved at tale med dem (og få dem til at tale med dig) kan du få øje på et problem og beskytte dem langt mere effektivt end nogen teknologi. Nogle yderligere trin omfatter:

Spil sikkert på nettet

- Kend til, hvilke spil de spiller og sørg for at spillene passer til dit barns alder.
- Begræns mængden af oplysninger, dine børn deler online. For eksempel bør de aldrig dele deres adgangskode, alder, telefonnummer eller hjemmeadresse.
- Overvej at have deres spillecomputer i et åbent område, hvor du kan holde øje med dem. Derudover bør yngre børn ikke spille på deres værelser eller sent om aftenen.
- Mobning, grimt sprog eller anden antisocial adfærd kan være et problem. Hold øje med dine børn, hvis de virker forstyrrede efter at have spillet et spil, de kan være blevet mobbet online. Hvis de bliver mobbet online, skal de stoppe med at spille spillet og spille i et mere børnevenligt miljø, eller få dem til at spille online-spil med betroede venner.
- Find ud af om dit barns spil understøtter køb i appen og hvilke former for forældrestyring de giver.

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

Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016
Social Engineering (oversat til dansk):	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases (oversat til dansk):	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Two-step Verification (oversat til dansk):	https://securingthehuman.sans.org/ouch/2015#september2015

Licensinformation

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