OUCH! | Juli, 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Sikre deg selv
- Sikre PC-en din
- For foreldre

Trygghet og sikkerhet ved nett-gaming

Oversikt

Nett-gaming er en flott måte å ha det moro på, men det kommer også med sitt eget sett med unike risikoer. I dette nyhetsbrevet går vi over hva du og familien din kan gjøre for å holde dere trygge når dere spiller dataspill over nettet.

Gjesteredaktør

Steve Armstrong grunnla Logically Secure, er en sertifisert SANS-instruktør, og er skaper av CyberCPR, en hendelseshåndteringsplatform. Han er aktiv på Twitter som **@Nebulator**, arbeider med mange store spillselskaper i hele verden, og lever ut gutte- og arbeidslivsdrømmen!

Sikre deg selv

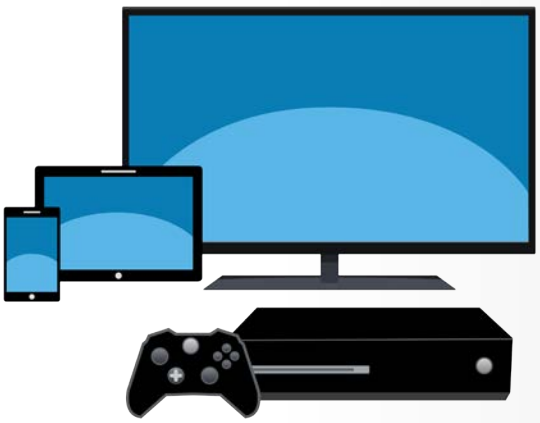
Det som gjør nett-gaming så moro er at du kan spille og kommunisere med andre fra hvor som helst i hele verden. Ganske ofte kjenner du ikke engang de du spiller med. Selv om det store flertallet av folk som spiller på nettet kun er ute etter å ha deg gøy, slik som deg, fins det noen som ønsker å gjøre skade. Her er noen grep du bør ta for å holde deg sikker:

- Vær forsiktig med en hver melding som ber deg utføre en spesiell handling, som å klikke på en link eller laste ned en fil. Akkurat som med phishing-angrep på e-post vil kriminelle forsøke å lure deg i spillene til å infisere datamaskinen din eller stjele identiteten din. Dersom en melding skaper følelse av hastverk, virker rar eller for god til å være sann, bør du være oppmerksom på at det kan være et angrepsforsøk.
- Mange nettspill har sine egne markeder der du kan bytte, kjøpslå og til og med kjøpe virtuelle varer. Akkurat som i virkeligheten finnes det svindlere i disse systemene som vil prøve å lure deg, og stjele pengene dine eller den virtuelle valutaen du har opparbeidet deg. Handle kun med folk som har etablerte gode rykter.
- Bruk sterke passordsetninger for enhver gaming-brukerkonto. På denne måten kan ikke angripere ganske enkelt gjette passordet ditt og ta over kontoen din. Ta i bruk to-trinns bekreftelse dersom spillet tilbyr det. I tillegg bør du sørge for at alle brukerkontoene dine har forskjellige passord. På den måten er de andre kontoene dine trygge selv om et spill skulle bli kompromittert. Om du ikke klarer å huske alle passordene dine burde du bruke et passordhåndteringsprogram.

Sikre systemet ditt

Kriminelle vil kanskje prøve å hacke seg inn i og ta over maskinen du spiller på, du må ta grep for å for å forsvare den:

Trygghet og sikkerhet ved nett-gaming



Nøkkelen til trygg nett-gaming er å bruke et sterkt passord, sikre datamaskinen din, og bruke sunn fornuft når du får rare meldinger og forespørsler.

- Sikre datamaskinen din ved å alltid kjøre siste versjon av operativsystem og spill. Gammel og utdatert programvare har kjente sårbarheter som angripere kan utnytte for å hacke inn på datamaskinen din. Ved å holde datamaskinen og spillene på den oppdatert, eliminerer du de fleste av disse kjente sårbarhetene.
- Bruk antivirus-programvare, sørg for at det er oppdatert og at det sjekker alle filene du kjører i sanntid.
- Last kun ned spill og spill-relatert programvare fra pålitelige nettsteder. Ofte vil cyberkriminelle lage en falsk og infisert versjon av spillet, som de så distribuerer fra sine egne servere eller fra torrent-nettsteder.
- Tilleggspakker og modifikasjoner laget av spillersamfunnet brukes ofte for å legge til nytt innhold i spill. Angripere kan av og til infisere disse spillpakkene med skadevare. Akkurat som med spill, sørg for at du også laster ned tilleggsinnhold kun fra pålitelige kilder. Om en tilleggspakke krever at du slår av antivirus-programmet eller gjør endringer i sikkerhetsinnstillingene, bør du ikke bruke den.
- Undergrunnsmarkeder har dukket opp for juksing i spill. I tillegg til å være uetiske, er mange jukseprogrammer egentlig skadevare som infiserer datamaskinen din. Aldri installer eller ta i bruk jukseprogrammer eller nettsider.
- Sjekk nettsiden til det du måtte bruke av nett-gaming programvare. Mange slike sider har egne seksjoner for å sikre deg selv og systemet ditt.
- Til slutt, vær alltid like forsiktig med spilling på mobile enheter som du ville vært med spilling på datamaskinen din. Cyberkriminelle har også begynt å rette seg mot mobile enheter.

For foreldre og foresatte

Barn trenger ekstra beskyttelse og opplæring når det er snakk om nett-gaming. Opplæring og en åpen dialog med barna dine er en av de mest effektive tiltakene du kan gjøre for å beskytte dem. En av våre favoritt-triks for å få barna til å åpne seg, er å spørre dem om hvordan spillet deres fungerer, få dem til å gå gjennom nett-verdenen og vise deg hvordan et typisk spill er. Kanskje til og med spill spillet sammen med dem. I tillegg kan du få dem til å beskrive de forskjellige folkene de møter over nettet. Ganske ofte kan nett-gaming være en stor del av det sosiale livet til barnet ditt. Ved å snakke med dem (og få dem til å snakke med deg) kan du oppdaga problemer og beskytte dem langt mer effektivt enn noen form for teknologi. I tillegg kan du ta noen av disse grepene:

Trygghet og sikkerhet ved nett-gaming

- Ha kjennskap til spillene de spiller, og vær trygg på at du føler at spillene passer til barnas alder.
- Begrens mengden informasjon barna deler på nettet. For eksempel burde de aldri dele passord, alder, telefonnummer eller adresse.
- Vurder å ha maskinen de spiller på i et åpent område hvor du kan holde et øye med dem. I tillegg burde ikke yngre barn spillet på rommet sitt sent om natten.
- Mobbing, stygt språk og andre antisosiale tendenser kan være et problem. Hold et øye med barna, virker de utafor etter et spill kan de ha blitt utsatt for mobbing. Hvis de blir mobbet i nettspill, kan du få dem til å slutte å spille spillet og heller spille i mer barnevennlige spillmiljøer, eller få dem til å kun spille med nære venner.
- Ha kjennskap til om barnets spill støtter kjøp i spillet, og hva slags foreldrestyring som er mulig.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

Slik sikrer du hjemmenettverket ditt:	https://securingthehuman.sans.org/ouch/2016#february2016
Sosial manipulering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passordsetninger:	https://securingthehuman.sans.org/ouch/2017#april2017
Passordhåndteringsprogrammer:	https://securingthehuman.sans.org/ouch/2015#october2015
Totrinns pålogging:	https://securingthehuman.sans.org/ouch/2015#september2015

Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS