OUCH! | Mars, 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Sikre deg selv
- Sikre datamaskiner / kontoer
- For foreldre

Spille på Internett sikkert

Oversikt

Spilling på nett er en god måte å ha det morsomt på, men det kommer også med noen unike risikoer. I dette nyhetsbrevet vil vi gå gjennom hva du kan gjøre for å beskytte deg selv og din familie når du spiller på nett.

Gjesteredaktør

Jake Williams er grunnlegger av og hovedkonsulent i Rendition Infosec, sertifisert SANS instruktør og medforfatter av flere SANS kurs. Han er aktiv på Twitter (**@MalwareJake**) og blogger regelmessig på **malwarejake.blogspot.com**.

Sikre deg selv

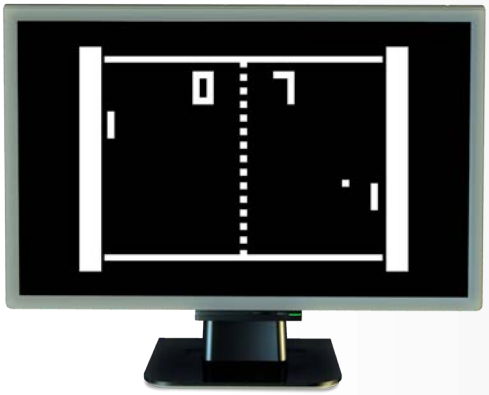
Noe av det som gjør spilling på nett så engasjerende er at du kan spille og kommunisere med andre personer fra andre steder i verden. Ofte vet du ikke en gang hvem du spiller med. De fleste av personene du møter er bare ute etter å ha det moro, akkurat som deg, men det er også de som vil gjøre skade. Her er noen ting du kan gjøre for å holde deg sikker.

- Vær varsom med beskjeder du får som ber deg begå en handling, som å klikke på en link eler laste ned en fil. Samme som med phishing-angrep, kriminelle vil prøve å lure deg til å foreta en handling som vil infisere maskinen din. Hvis beskjeden virker merkelig, gir en følelse av hast eller at det rett og slett virker for godt til å være sant, vær mistenksom og gå ut i fra at det er et angrep.
- Flere spill har et eget pengesystem der du kan bytte og kjøpe virtuelle valutaer. Akkurat som i den virkelige verden finnes det svindlere som vil prøve å lure deg til å gi fra deg penger eller stjele pengene dine direkte.
- Vær forsiktig når du utfører transaksjoner der ekte penger er brukt for å kjøpe goder i spillet og motsatt. Sjekk at markedet har et godt rykte før du utfører slike transaksjoner.
- Begrens informasjonen du eller barna dine deler på nett, du bør aldri dele informasjon som passord eller bostedsadresse.
- Mange nettsteder, som nettbanken, bruker sikkerhetsspørsmål for å bekrefte din identitet. En kjent metode blant angripere er å gjette disse spørsmålene ved å ta kontakt med offeret via spill på nett. Husk at du ikke trenger å svare på spørsmål som kommer fra andre når du spiller på nett.

Spille på Internett sikkert

Sikre datamaskiner / kontoer

Det neste steget er å sikre datamaskinen du bruker. Kriminelle vil prøve å ta over datamaskinen eller kontoer, under er noen steg du bør ta for å beskytte dem.



Nøkkelen til å sikre seg når man spiller på nett er å bruke sterke passord, sikre datamaskinen og bruke sunn fornuft når du snakker med fremmede eller når du mottar merkelige beskjeder eller henvendelser.

- Bruk et sterkt passord, både for datamaskinen og for kontoer på nett. Hvis du gjør dette, så unngår du at angripere gjetter passordet og tar over kontoen på den måten. Hvis to-steg verifisering er støttet, ta det i bruk. Du bør også sørge for at hver konto har forskjellige passord, dermed unngår du at kompromittering av en konto fører til at andre kontoer blir kompromittert.
- Sørg for at du sikrer datamaskinen ved å alltid kjøre siste versjon av operativsystemet og spillet. Akkurat som med operativsystemet og nettlesere, eldre versjoner av spillet har ofte kjente svakheter som angripere kan utnytte og bruke for å kompromittere datamaskinen. Ved å holde datamaskinen og spillet oppdaterte eliminerer du mesteparten av disse svakhetene.
- Bruk antivirus og sørg for at det er oppdatert og sjekker filer i sanntid.
- Last kun ned spill fra nettsider du stoler på. Hvis du installerer et program for å spille et spill, sørg for at du laster det ned fra leverandørens nettside eller fra en annen leverandør du stoler på. Ofte vil angripere lage falske eller infiserte versjoner av et spill og deretter distribuere det fra deres server. Hvis du installerer et av disse programmene vil angripere kunne ta full kontroll over datamaskinen din.
- Utvidelser til spill, ofte utviklet av andre brukere, kan brukes til å legge til nye funksjoner. Angripere infiserer noen ganger disse utvidelsene med virus som kan være veldig vanskelig for antivirus å oppdage. Akkurat som når du laster ned spill, sørg for at du laster ned utvidelsen fra en lokasjon du stoler på. I tillegg, hvis utvidelsen krever at du deaktiverer antiviruset eller gjør forandringer i brannmuren, ikke bruk det.
- Det finnes egne svarte markeder for å støtte jukseaktivitet. I tillegg til at det er uetisk, er mange programmer som bistår med juksing rootkits, den farligste formen for virus. Ikke installer eller bruk programmer som bistår med å jukse.
- Sjekk ut hjemmesiden til spillet du spiller. Mange spilleverandører bruker en del av siden til å forklare hvordan du kan beskytte deg selv, sørg for at du følger tipsene de gir.

Spille på Internett sikkert

- Det er like viktig at du er forsiktig når du spiller på mobile enheter som når du spiller på datamaskinen. Angripere angriper mobile enheter også.

For foreldre

Hvis du er forelder til et barn, sørg for at barnet følger stegene gitt ovenfor (for unge barn må du kanskje utføre noen av disse stegene for dem). Det er også viktig at du kommuniserer med barna og forklarer risikoene. Opplæring og åpen kommunikasjon er et av de mest effektive stegene kan ta for å beskytte dem. Ett steg for å få barna til å snakke, er å be de om å vise deg hvordan spillet fungerer, få dem til å gå gjennom verdenen i spillet og vise hvordan et typisk spill ser ut. Kanskje du også kan spille spillet sammen med dem. Be de også beskrive de forskjellige personene de møter i spillet, ofte er spilling på nett en stor del av det sosiale livet til barnet. Ved å snakke med barnet (og få de til å snakke med deg) kan du lettere se mulige problemer og du kan beskytte dem mer effektivt enn noe annen teknologi.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos
http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

Sosial manipulering:	http://www.securingthehuman.org/ouch/2014#november2014
Phishing angrep:	http://www.securingthehuman.org/ouch/2013#february2013
Passord:	http://www.securingthehuman.org/ouch/2013#october2013
Hva er antivirus?:	http://www.securingthehuman.org/ouch/2014#december2014
StaySafe Online:	http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis