SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Luglio 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Giochi online e sicurezza

Introduzione

I giochi online sono molto divertenti, ma sono anche caratterizzati da alcuni rischi peculiari. In questa newsletter illustreremo ciò che tu e la tua famiglia potete fare per proteggerti quando giochi online.

L'autore di questo numero

Steve Armstrong è il fondatore di Logically Secure, un istruttore SANS certificate e architetto di CyberCPR, una piattaforma di Incident Management. È attivo su Twitter come **@Nebulator** e lavora con molte aziende produttrici di giochi, realizzando così i suoi sogni di bambino e di professionista della sicurezza.

Come proteggersi

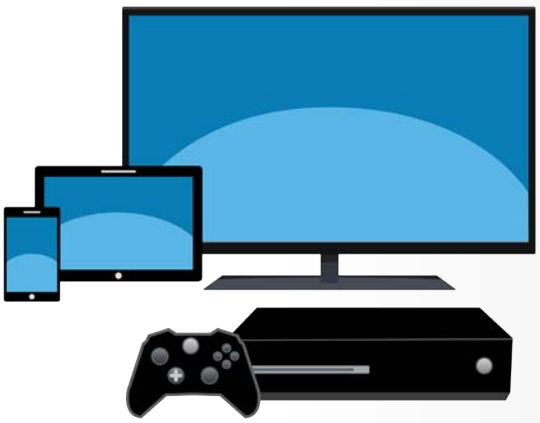
Ciò che rende il gioco online così divertente è che puoi giocare e comunicare con persone da qualsiasi parte del mondo, spesso senza neanche conoscerli. Sebbene la stragrande maggioranza dei giocatori online ci comporta come te, ci sono purtroppo alcuni che partecipano per scopi malevoli. Ecco alcune indicazioni da seguire per aumentare la tua sicurezza.

- Presta attenzione a qualsiasi messaggio che ti chiede di intraprendere un'azione, ad esempio cliccando su un collegamento o scaricando un file. Proprio come negli attacchi di phishing di posta elettronica, i malfattori tentano di ingannarti anche nei giochi online per farti compiere azioni che possono infettare il computer o permettere la sottrazione della tua identità. Se il contenuto di un messaggio sembra strano, urgente o troppo bello per essere vero, può trattarsi di un attacco.
- Molti giochi online hanno i loro mercati finanziari in cui scambiare, barattare o anche acquistare beni virtuali. Proprio come nel mondo reale, in questi sistemi ci sono truffatori che cercheranno di ingannarti e rubare i tuoi soldi o la valuta virtuale che hai accumulato. Fai affari solo con persone che hanno una reputazione attendibile.
- Utilizza una passphrase forte per ogni account di gioco. In questo modo gli aggressori non potranno indovinare le tue password per accedere agli account. Se il gioco offre la verifica in due passaggi, utilizzala. Fai anche in modo che ogni account online abbia una password diversa. In questo modo, se un gioco verrà compromesso, gli altri account saranno al sicuro. Non riesci a ricordare tutte le tue password? Prendi in considerazione un Password manager.

Rendere sicuro il computer

I malintenzionati potrebbero tentare di hackerare il computer su cui stai giocando, per cui è necessario intervenire per proteggerlo.

Giochi online e sicurezza



Per giocare online in modo sicuro è necessario usare password forti, proteggere il computer e, quando si ricevono messaggi o richieste strane, usare il buon senso.

- Proteggi il computer utilizzando la versione più recente del sistema operativo e del software di gioco. Il software vecchio e obsoleto ha vulnerabilità conosciute che gli hacker possono sfruttare per attaccare il computer. Aggiornando le applicazioni e i giochi, eliminerai la maggior parte delle vulnerabilità note.
- Utilizza software antivirus, assicurati che sia aggiornato e impostalo per controllare i programmi in esecuzione in tempo reale.
- Scarica software di gioco solo da siti web attendibili. Molto spesso i cyber criminali creano una versione falsa o infettata di un gioco, per poi distribuirlo dal proprio server.
- I pacchetti aggiuntivi, spesso sviluppati dalla comunità, vengono utilizzati per aggiungere nuove funzionalità al gioco, ma gli hacker talvolta infettano questi pacchetti con del malware. Proprio come fa quando scarichi giochi, assicurati di scaricare anche i componenti aggiuntivi da siti di fiducia. Inoltre, se qualsiasi componente aggiuntivo richiede di disattivare l'anti-virus o apportare modifiche alle impostazioni di protezione, non utilizzarlo.
- Nel tempo sono stati creati molti mercati underground per permettere ai giocatori di usare trucchi per "barare" (cheat). Oltre a non essere etici, molti programmi di questo tipo contengono malware in grado di infettare il computer. Non installare né utilizzare alcun tipo di software per barare.
- Controlla il sito web relativo a qualsiasi software di gioco online che utilizzi. Molti siti di gioco hanno una sezione dedicata alla sicurezza.
- Infine, fai sempre attenzione quando giochi con i tuoi dispositivi mobili. Gli attacchi cyber stanno cominciando a puntare anche su tablet e smartphone.

Per genitori e tutori

I bambini hanno bisogno di protezione e istruzioni ulteriori quando giocano online. Queste istruzioni, insieme a un dialogo aperto con i propri figli, sono le azioni più efficaci che potete intraprendere per proteggerli. Uno dei nostri trucchi preferiti per far parlare i ragazzi è chiedere di mostrarvi come funzionano i loro giochi, "accompagnarvi" nel loro mondo online e giocare con loro. Chiedete inoltre di descrivervi le diverse persone che incontrano online. Molto spesso il gioco può costituire una parte importante della vita sociale del vostro bambino. Parlando con loro (e facendo in modo che parlino con voi) è possibile individuare i problemi e proteggerli in modi più efficace di qualsiasi tecnologia. Ecco altre azioni che vi potranno aiutare:

Giochi online e sicurezza

- Sapere quali giochi stanno usando i vostri figli e assicurarsi che i giochi siano appropriati per la loro età.
- Limitare la quantità di informazioni che i bambini condividono online. Ad esempio, non dovrebbero mai condividere la propria password, l'età, il numero di telefono o l'indirizzo di casa.
- Collocate il computer di gioco in un'area in cui potete tenerli d'occhio. I bambini più piccoli non dovrebbero giocare nelle loro camere o fino a tarda notte.
- Il bullismo, il turpiloquio o gli altri comportamenti antisociali possono essere un problema. Tenete d'occhio i vostri figli, se sembrano sconvolti dopo aver giocato una partita in cui possono essere diventati vittime di bullismo. Se questo succede, fate interrompere il gioco e fateli giocare in ambiti più adatti ai bambini o solo con amici fidati.
- Verificate se i giochi dei vostri figli supportano gli acquisti in-app e quali tipi di controlli parentali offrono.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Proteggere la rete di casa:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_it.pdf
Il Social Engineering:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_it.pdf
Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_it.pdf
I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
La verifica in due passaggi:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf

Direzione editoriale: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley