SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Marzo 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Giochi online e sicurezza

Introduzione

Per molti, i giochi online sono una fonte di vero divertimento che però, purtroppo, si accompagna a una tipologia peculiare di rischi. In questa newsletter, illustreremo cosa potete fare per proteggere voi stessi e la vostra famiglia anche negli ambienti di gioco online.

L'autore di questo numero

Jake Williams è fondatore e consulente di Rendition Infosec, istruttore SANS certificato e coautore di vari corsi. Potete seguirlo su Twitter come **@MalwareJake** e sul suo blog **malwarejake.blogspot.com**.

La vostra sicurezza

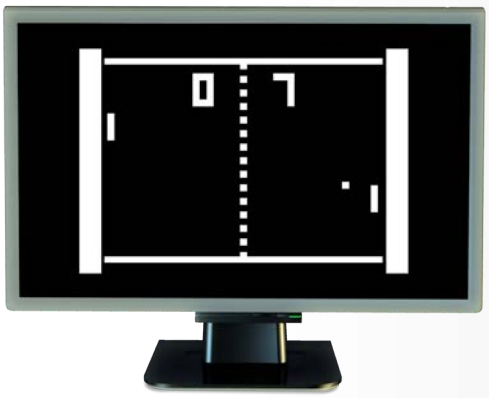
Ciò che rende i giochi online così coinvolgenti è la possibilità di giocare e comunicare con altri in qualsiasi parte del mondo, spesso senza nemmeno conoscerne l'identità. Mentre la maggior parte dei giocatori online cerca solo il puro divertimento, esiste una categoria di persone che vuole invece trarre un vantaggio a scapito di altri. Ecco alcune cose che dovreste sapere.

- Fate attenzione ai messaggi che vi chiedono di fare qualcosa come cliccare su un link o scaricare un file. Proprio come per gli attacchi di phishing, i criminali informatici tenteranno di ingannarvi per farvi compiere un'azione che porterà il vostro computer a infettarsi. Se un messaggio vi appare sospetto, vi sollecita con urgenza o è troppo bello per essere vero, potrebbe trattarsi di un attacco.
- Molti giochi online hanno un mercato finanziario proprio dove potete effettuare scambi, baratti o comprare beni virtuali. Proprio come nel mondo reale, anche in questi contesti esistono truffatori che possono tentare di sottrarvi del denaro.
- Fate attenzione quando effettuate transazioni con denaro reale per comprare beni all'interno di un gioco. Fatelo solo in mercati che godono di una buona reputazione.
- Limitate il numero di informazioni che voi e i vostri figli condividete online. Non condividete mai informazioni personali dettagliate, come la vostra password o l'indirizzo di casa.
- Molti siti web, come quelli di e-banking, usano domande di sicurezza per confermare la vostra identità. I truffatori riescono a ottenere le risposte a queste domande diventando amici delle loro vittime nei giochi online. Ricordate che non avete alcun obbligo di rispondere alle domande che vi vengono poste in un gioco.

Giochi online e sicurezza

La sicurezza di computer e account

Il passo successivo è di rendere sicuro il computer che state usando. Gli imbroglioni cercheranno di prendere il possesso del vostro computer o del vostro account di gioco, per cui sta a voi proteggervi al meglio.



Il modo migliore per aumentare la sicurezza quando giocate online è di usare password forti, rendere sicuro il computer e usare il buon senso quando parlate con estranei o ricevete messaggi sospetti.

- Usate una password forte sia per il vostro computer sia per i vostri account. In questo modo, un attaccante non riuscirà a indovinarla. Se il gioco offre la possibilità di usare la verifica in due fattori, fatene uso. Inoltre, assicuratevi che ognuno dei vostri account abbia una password diversa, in modo che se un gioco venisse compromesso, gli altri account siano al sicuro.
- Rendete sicuro il vostro computer aggiornandolo sempre all'ultima versione del sistema operativo e del software di gioco. Proprio come il sistema operativo e il browser, un software di gioco non aggiornato ha spesso vulnerabilità conosciute che gli hacker possono sfruttare per prendere possesso del vostro computer. Mantenendolo aggiornato, eliminerete la maggior parte di queste vulnerabilità.
- Usate un anti-virus, aggiornatelo e impostatelo per controllare in tempo reale ogni programma che eseguite.
- Scaricate il software di gioco solo da siti web affidabili. Se state installando del software, assicuratevi prima di averlo scaricato dal sito del produttore o da un altro sito di cui avete fiducia. Molto spesso i criminali informatici creano una versione falsa o infetta del gioco, e lo distribuiscono dai loro server. Se installate una di queste versioni, i criminali avranno il completo controllo del vostro computer.
- I componenti aggiuntivi, spesso sviluppati dalle community di un gioco, sono frequentemente utilizzati per introdurre nuove funzionalità. Gli hacker a volte infettano questi componenti con malware che risulta molto difficile da individuare, anche per un anti-virus. Proprio come fate quando scaricate i giochi, anche nel caso dei download di componenti aggiuntivi dovete porre molta attenzione e farlo solo da siti di fiducia. Inoltre, se un componente richiede di disabilitare l'anti-virus, o di apportare modifiche al firewall, non usatelo.
- Anche in questo mondo esiste un mercato nero dedicato alle modalità di barare nel gioco (cheating). Oltre a essere poco etici, molti programmi usati per questi scopi sono dei rootkit, il tipo di malware più pericoloso. Non installate nessun tipo di software per barare.
- Controllate il sito web del software di gioco che state usando: molti siti hanno sezioni che illustrano come proteggervi. Fate tesoro dei consigli che danno.

Giochi online e sicurezza

- Infine, ponete la stessa attenzione anche ai vostri dispositivi mobili, poiché costituiscono la nuova frontiera degli attacchi informatici.

Per i genitori

Se siete genitori, assicuratevi che i vostri figli seguano le indicazioni illustrate precedentemente (per i bambini più piccoli, dovreste essere voi a farlo). Parlate con loro di questi rischi: l'educazione e il dialogo aperto con i bambini è uno dei metodi più efficaci che possiate adottare per proteggerli. Uno dei trucchi per far parlare i bambini è chiedere di illustrarvi come funzionano i loro giochi, farvi accompagnare attraverso il loro mondo online e giocare con loro. Fateli anche parlare delle persone che incontrano online. Spesso il gioco online è una parte importante della vita sociale dei vostri figli: parlando con loro, e facendo in modo che loro parlino con voi, sarete in grado di individuare i problemi e proteggerli in modo molto più efficace di qualsiasi tecnologia.

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
http://www.securingthehuman.org

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

Social Engineering:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf
Attacchi di Phishing:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_it.pdf
Le password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
Cos'è un anti-virus?:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis