OUCH! | Marzec 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- Zabezpieczenie siebie
- Zabezpieczenie swojego komputera i konta
- Dla rodziców

Bezpieczne granie online

Wstęp

Gry online są świetną zabawą, ale też niosą ze sobą specyficzne rodzaje ryzyka. W tym wydaniu omawiamy w jaki sposób możesz nie narażać siebie i swojej rodziny gdy grasz online.

Redaktor gościnny

Jake William jest twórcą i głównym konsultantem w firmie Rendition Infosec, certyfikowanym instruktorem SANS, współautorem kilku kursów instytutu SANS. Jest aktywny na Twitterze jako **@MalwareJake** i prowadzi bloga **malwarejake.blogspot.com**.

Zabezpieczenie siebie

Jednym z powodów, dla którego gry online są tak popularne jest fakt, że pozwalają grać i rozmawiać z innymi graczami z całego świata. Często możesz nawet nie znać osób, z którymi grasz. O ile większość graczy szuka tylko dobrej zabawy, to są też tacy, którzy chcą wyrządzić Ci krzywdę. O to kilka wskazówek, które pozwolą Ci czuć się bezpiecznie.

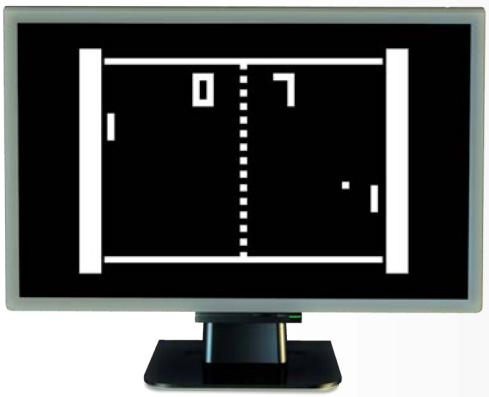
- Zwracaj uwagę na wiadomości, które wymagają od Ciebie podjęcia akcji takich jak na przykład kliknięcie w link czy pobranie pliku. Tak jak w przypadku ataków typu phishing, ktoś może próbować Ciebie namówić do zainfekowania swojej maszyny. Jeśli wiadomość wydaje się dziwna, pilna czy zbyt nieprawdopodobna to najlepiej ją zignorować.
- Wiele gier online tworzy własne ekonomie, gdzie możesz wymieniać się czy nawet kupować wirtualne dobra. Tak jak i w życiu, podstępni ludzie chcą wykorzystać Ciebie i ukraść Ci pieniądze lub przedmioty z gry.
- Zwracaj szczególną uwagę na transakcje, które związane są z prawdziwymi pieniędzmi. Pamiętaj, aby kupować i sprzedawać tylko na oficjalnych stronach gry.
- Ograniczaj ilość informacji, które Ty lub twoje dzieci publicznie udostępniacie. Nigdy nie dziel się informacjami prywatnymi takimi jak hasło czy adres domowy.
- Dużo stron, jak np. serwisy bankowe, używa pytań, aby potwierdzić twoją tożsamość. Atakujący potrafią wydobyć takie informacje zaprzyjaźniając się z graczami. Pamiętaj, że nie masz żadnego obowiązku odpowiadania na pytania zadawane Ci podczas gry.

Zabezpieczenie swojego komputera i konta

Kolejnym krokiem jest zabezpieczenie używanego przez Ciebie komputera. Atakujący będą się starali zdobyć kontrolę nad Twoim komputerem i kontami, dlatego musisz się przed tym chronić.

Bezpieczne granie online

- Używaj mocnych haseł zarówno do komputera jak i do kont w grach online. W ten sposób atakujący nie zgadną łatwo hasła, przejmując w ten sposób konto. Jeśli gra oferuje dwuskładnikowe uwierzytelnianie to pamiętaj, aby je włączyć. W dodatku upewnij się, że różne konta, które posiadasz mają różne hasła. W ten sposób jeśli nastąpi włamanie na serwer jednej z gier, pozostałe Twoje konta wciąż pozostaną bezpieczne.
- Zabezpiecz swój komputer używając zawsze jak najnowszej wersji systemu operacyjnego oraz gry. Tak samo jak w przypadku starszych wersji systemu operacyjnego czy przeglądarki internetowej, starsza wersja gry może zawierać znane atakującym podatności, które mogą być wykorzystane do przejęcia kontroli nad Twoim komputerem. Dbając o aktualność gry jak i innych aplikacji pozbywasz się tych podatności.
- Uruchom program antywirusowy, sprawdź czy używasz jego najnowszej wersji i włącz skanowanie w czasie rzeczywistym.



Kluczem do pozostania bezpiecznym podczas grania online jest użycie silnych haseł, zabezpieczenie komputera i użycie zdrowego rozsądku przy rozmowach z obcymi lub gdy dostajemy dziwne wiadomości lub prośby.

- Pobieraj gry tylko z zaufanych stron. Jeśli instalujesz grę pobierz ją z oficjalnej strony producenta, albo z innej zaufanej strony. Dosyć często zdarza się, że przestępcy tworzą własną, zainfekowaną wersję gry i dystrybuują ją korzystając ze swojego serwera. Jeśli zainstalujesz taką wersję, atakujący mogą przejąć kontrolę nad Twoim komputerem.
- Dodatki do gier, często tworzone przez społeczność graczy, dodają nowe funkcjonalności do już istniejącej wersji. Atakujący czasem infekują te dodatki złośliwym oprogramowaniem co może okazać się trudne do wykrycia, nawet przez program antywirusowy. Upewnij się, że pobierasz dodatki z zaufanej strony. Jeśli któryś z nich wymaga wyłączenia antywirusa albo zapory sieciowej to po prostu go nie instaluj.
- Powstało wiele nielegalnych serwisów, aby pomóc w oszukiwaniu w grach. Poza stroną etyczną takich działań, często programy wspomagające graczy są rootkitami - jedną z najgroźniejszych form złośliwego oprogramowania. Nigdy nie instaluj ani nie używaj programów służących do oszukwiania w grach.
- Sprawdź informacje zawarte na stronie internetowej gry. Wiele stron zawiera sekcję z informacjami na temat Twojego bezpieczeństwa i Twojej maszyny. Skorzystaj z tych porad.
- W końcu pamiętaj, aby stosować te same środki ostrożności grając w grę na komputerze jak i na telefonie komórkowym. Atakujący obierają także za cel urządzenia mobilne.

Bezpieczne granie online

Dla rodziców

Jeśli jesteś rodzicem to upewnij się, że Twoje dzieci stosują się do powyższych zaleceń (w przypadku młodszych dzieci być może będziesz musiał wykonać część kroków za nie). Porozmawiaj także z dziećmi o ryzykach związanych z grami online. Edukacja i otwarty dialog to jedne z najlepszych sposobów na zachowanie bezpieczeństwa. Jednym z najlepszych sposobów na rozpoczęcie takiej rozmowy jest poproszenie dziecka o pokazanie gry, włączając w to cały świat z nią związany jak i obejrzenie samej rozgrywki. Można nawet spróbować włączyć się do gry. Niech dzieci również opiszą inne osoby, z którymi spotykają się online. Często spotkania w grach mogą odgrywać duże znaczenie w życiu społecznym Twoich dzieci. Rozmawiając z nimi o tym można szybciej zauważyć problem i na niego odpowiednio wcześnie zareagować nawet bez pomocy ze strony różnych technologii.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Przydatne linki

Socjotechnika: http://www.securingthehuman.org/ouch/2014#november2014
Email i ataki phishingowe: http://www.securingthehuman.org/ouch/2013#february2013
Systemy zarządzania hasłami: http://www.securingthehuman.org/ouch/2013#october2013
Czym jest antywirus?: http://www.securingthehuman.org/ouch/2014#december2014
Bezpieczeństwo dzieci online: Kompendium dla rodziców i profesjonalistów:
http://www.saferinternet.pl/images/artykuly/projekty-edukacyjne/Kompendium_www.pdf

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski