OUCH! | Lipiec, 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Zadbaj o własne bezpieczeństwo
- Zabezpiecz swój komputer
- Kilka słów dla rodziców

Gry Online - bezpieczeństwo

Wprowadzenie

Gry online to wspaniały sposób na dobrą zabawę, pociągają jednak za sobą pewne ryzyko. W bieżącym wydaniu biuletynu OUCH! opowiemy, co możesz zrobić dla siebie i Twojej rodziny w celu poprawy bezpieczeństwa podczas grania online.

Redaktor gościnny

Steve Armstrong jest założycielem Logically Secure, certyfikowanym instruktorem SANS oraz twórcą platformy zarządzania incydentami CyberCPR. Dostępny na Twitterze jako **@Nebulator**. Współpracuje z wieloma znanymi wytwórniami gier, realizując w ten sposób marzenia z dzieciństwa i aspiracje zawodowe!

Zadbaj o własne bezpieczeństwo

W internetowych rozgrywkach niezwykle fascynujące jest to, że możesz nawiązać kontakt i zaprosić do gry osoby z dowolnej części świata. Bardzo często nie znamy graczy, z którymi podejmujemy rywalizację. Podczas gdy zdecydowana większość z nich bierze udział w rozgrywkach, aby tak jak Ty dobrze się bawić, niektóre osoby korzystają z powyższych serwisów, aby wyrządzić innym szkodę. Poniżej podajemy kilka dobrych praktyk, które warto podjąć, aby pozostać bezpiecznym:

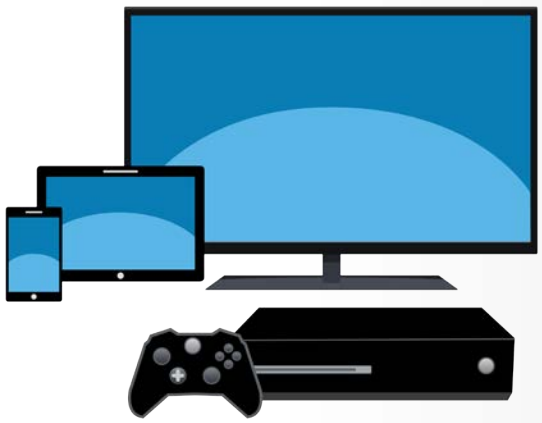
- Bądź wyczulony na wszelkie wiadomości, zachęcające do podejmowania działań, takich jak kliknięcie w link czy pobranie pliku. Podobnie jak w przypadku wiadomości e-mail zawierających phishing, oszuści będą próbowali zachęcić Cię do aktywności, które mogą zainfekować Twój komputer lub ukraść Twoją tożsamość. Jeśli wiadomość wygląda nienaturalnie, sprawia wrażenie pilnej, lub mało wiarygodnej z uwagi na obietnicę łatwego zysku, powinna wzbudzić Twoje podejrzenia.
- Wiele internetowych serwisów dla graczy posiada swoje własne sklepy, w których możesz sprzedawać, wymieniać i nabywać wirtualne towary. Podobnie jak w realnym świecie, są tam obecni oszuści. Będa oni próbowali oszukać Cię, chcąc ukraść Twoje pieniądze lub zgromadzoną wirtualną walutę. Przeprowadzaj transakcje tylko z zaufanymi osobami, których reputacja jest wiarygodna.
- Dla każdego konta w portalu dla graczy przygotuj odpowiednio trudne do złamania hasło. Dzięki temu atakujący nie będą mogli łatwo go odgadnąć i przejąć w ten sposób Twojego konta. Jeżeli jakiś serwis umożliwia zastosowanie dwuskładnikowego uwierzytelniania, skorzystaj z tego rozwiązania. Pamiętaj, aby nie używać takich samych haseł do różnych kont – jeżeli jedno z nich zostanie przejęte, pozostałe także nie będą bezpieczne. Abyś nie musiał zapamiętywać danych logowania do wszystkich kont, rozważ skorzystanie z aplikacji będącej menedżerem haseł.

Zabezpiecz swój komputer

Wrogo nastawione osoby mogą podejmować próby włamań i przejęcia dostępu do Twojego komputera, dlatego warto podjąć pewne kroki, które pomogą zachować bezpieczeństwo.

Gry Online - bezpieczeństwo

- Chroń swój komputer korzystając z aktualnych wersji systemu operacyjnego i oprogramowania do gier. Przestarzałe i nieaktualne oprogramowanie posiada znane podatności, które atakujący mogą wykorzystać, chcąc uzyskać nieuprawniony dostęp do Twojego komputera. Instalując bieżące aktualizacje, wyeliminujesz wiele z tych podatności.
- Korzystaj z antywirusa, upewnij się, że jest aktualny, posiada bieżące sygnatury wirusów oraz weryfikuje wszystkie otwierane przez Ciebie pliki.
- Aplikacje dla graczy pobieraj tylko z zaufanych źródeł. Nierzadko cyberprzestępcy przygotowują fałszywą lub zainfekowaną wersję gry, którą dystrybuują za pośrednictwem własnych serwerów.
- Dodatki do gier, często rozwijane przez społeczność, służą do nadawania nowych funkcjonalności. Zdarza się, że atakujący infekują te dodatki złośliwym oprogramowaniem. Podobnie jak podczas pobierania gier, upewnij się, że pobrałeś dodatek z zaufanej lokalizacji. Dodatkowo, jeżeli jakakolwiek aplikacja wymaga od Ciebie wyłączenia antywirusa, lub zmian w polityce bezpieczeństwa – nie używaj jej.



Kluczem do bezpiecznego grania online jest korzystanie z silnych haseł, zabezpieczenie swojego komputera i zachowanie zdrowego rozsądku w sytuacji otrzymania podejrzanych wiadomości lub żądań.

- Rynek podziemia powstał, aby wspierać nieuczciwe zachowania. Poza tym, że jest nieetyczny, wiele aplikacji służących oszustwom zawiera złośliwy kod, którego zadaniem jest zainfekować Twój komputer. Nigdy nie instaluj, ani nie odwiedzaj „cheaterskich" stron internetowych i oprogramowania.
- Zapoznaj się ze witryną internetową platformy do gier, której używasz. Wiele serwisów dla graczy posiada sekcję poświęconą bezpieczeństwu.
- Na koniec, bądź ostrożny pobierając gry na swoje urządzenia mobilne – one także są celem atakujących.

Dla rodziców i opiekunów

Dzieci wymagają szczególnej ochrony i edukacji w zakresie gier online. Edukacja i postawa dialogu z Twoim dzieckiem to jedne z najbardziej efektywnych kroków, jakie możesz podjąć, chcąc zapewnić im bezpieczeństwo. Jedna z naszych ulubionych sztuczek, aby dzieci coś opowiedziały, polega na poproszeniu ich, aby same zaprezentowały jak funkcjonuje świat gier. Pozwól im poprowadzić się przez wirtualny świat i pokazać na czym polega gra. A może zagracie wspólnie? Niech Twoje dzieci opowiedzą o osobach, które poznały w sieci. Dość często gry online stanowią znaczną część ich życia społecznego. Rozmawiając z nimi (i mając pewność, że one rozmawiają z Tobą) możesz naświetlić problem i ochronić je znacznie pewniej, niż korzystając z technologii. Poniżej podajemy kilka dodatkowych kroków, jakie możesz podjąć:

- Dowiedz się w jakie gry grają Twoje dzieci, upewnij się że są odpowiednie dla ich wieku.
- Ogranicz ilość informacji udostępnianych przez Twoje dziecko w sieci. Dla przykładu, nie powinno nigdy udostępniać swoich haseł, wieku, numeru telefonu, adresu zamieszkania.

Gry Online - bezpieczeństwo

- Umieszczenie komputera w widocznej przestrzeni to łatwiejszy sposób na weryfikację treści z jakich korzysta dziecko. Zwracaj uwagę, aby młodsze dzieci nie grały w swoich pokojach oraz późno w nocy.
- Nękanie, obelżywy język czy inne antyspołeczne zachowania mogą stanowić poważny problem. Obserwuj zachowanie swoich dzieci, jeżeli po skończonej zabawie online wyglądają na zdenerwowane, może to świadczyć że padły ofiarą negatywnych zachowań. W przypadku stwierdzenia cyberprzemocy, podejmij decyzję o zaprzestaniu korzystania z danej platformy lub aplikacji i poszukaj z dzieckiem czegoś bardziej przyjaznego. Być może rozwiązaniem będzie zabawa online ograniczona do grona zaufanych przyjaciół.
- Zweryfikuj czy gry, z których korzystają Twoje dzieci umożliwiają zakupy z poziomu aplikacji i jakiego rodzaju ograniczenia rodzicielskie oferują.

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 securingthehuman.sans.org/ouch/archives 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

Źródła

Bezpieczeństwo sieci domowych:	https://securingthehuman.sans.org/ouch/2016#february2016
Inżynieria społeczna:	https://securingthehuman.sans.org/ouch/2017#january2017
Silne hasła:	https://securingthehuman.sans.org/ouch/2017#april2017
Menedżery haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Dwuskładnikowe uwierzytelnianie:	https://securingthehuman.sans.org/ouch/2015#september2015

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

