

OUCH! Czerwiec 2022

Biuletyn Bezpieczeństwa Komputerowego

**Bezpieczne gry online**

To, co sprawia, że gry online są tak powszechne, to fakt, że można grać i wchodzić w interakcje z innymi osobami z dowolnego miejsca na świecie. Często nawet nie zna się ludzi, z którymi się gra. Podczas gdy zdecydowana większość ludzi w Internecie robi to dla rozrywki, zdarzają się osoby, które chcą wyrządzić krzywdę innym.

**Bądź bezpieczny**

Największym zagrożeniem gier online nie jest sama technologia, ale interakcje z nieznajomymi.

* Uważaj na wiadomości z prośbą o podjęcie działania, takiego jak kliknięcie łącza lub pobranie pliku. Atakujący mogą wykorzystywać wiadomości w grze lub wiadomościach phishingowych, aby nakłonić Cię do podjęcia działań, które mogą zainfekować Twój komputer lub przejąć dane. Jeśli wiadomość wydaje się dziwna, wymaga natychmiastowej reakcji lub po prostu jest zbyt piękna, aby była prawdziwa, należy podejrzewać, że może to być atak.
* Wiele gier online ma własne rynki finansowe, na których można handlować, wymieniać lub kupować wirtualne towary. Podobnie jak w prawdziwym życiu, są oszuści, którzy będą próbować cię oszukać i ukraść twoje pieniądze lub wirtualną walutę, którą posiadasz. Rozmawiaj tylko z zaufanymi osobami.
* Używaj silnego, unikalnego hasła do każdego konta do gry. W ten sposób atakujący nawet jeśli pozyskają jedno hasło do konta, nie będą w stanie przejąć innych kont. Jeśli dostawca gry/platformy wdrożył weryfikację dwuetapową, skorzystaj z niej. Masz trudności z zapamiętaniem haseł? Skorzystaj z menedżera haseł.

**Zabezpieczanie systemu**

Atakujący mogą próbować włamać się na konto lub przejąć kontrolę nad urządzeniem, z którego korzystasz. Musisz podjąć odpowiednie kroki, aby je ochronić.

* Pamiętaj o aktualizacji systemu operacyjnego i oprogramowania do najnowszych wersji. Nieaktualne oprogramowanie może posiadać luki w zabezpieczeniach, które atakujący wykorzystują. Jeśli to możliwe, korzystaj z automatycznych aktualizacji. Poprzez wgrywanie aktualizacji eliminujesz większość znanych luk w zabezpieczeniach.
* Pobieraj oprogramowanie i dodatki do gier tylko z zaufanych i oficjalnych źródeł. Atakujący często tworzą fałszywe lub zainfekowane wersje, a następnie rozpowszechniają je z własnego serwera. Ponadto, jeśli jakakolwiek gra lub dodatek wymaga wyłączenia jakichkolwiek zabezpieczeń lub zmianę ustawień, nie używaj ich.
* Pojawiły się rynki, które wspierają tego typu oszustwa. Oprócz tego, że są nieetyczne, wiele programów to złośliwe oprogramowanie, które może zainfekować urządzenie, z którego korzystasz. Nigdy nie instaluj ani nie używaj żadnego oprogramowania i nie korzystaj ze stron internetowych, które mogą służyć do nadużyć.
* Weryfikuj każdą witrynę do gier online, z której korzystasz. Wiele witryn z grami zawiera informacje o tym, jak zabezpieczyć system i chronić siebie.

**Dla rodziców lub opiekunów**

Edukacja i otwarty dialog z dziećmi to najskuteczniejszy krok, jaki możesz podjąć, aby je uchronić. Jednym ze sposobów jest poproszenie ich o pokazanie, jak działają ich gry i jak wygląda typowa rozgrywka. Dobrym pomysłem jest zagranie razem z dzieckiem. Ponadto poproś ich o opisanie osób, które spotykają w Internecie. Gry online mogą stanowić dużą część życia towarzyskiego Twojego dziecka. Przez rozmowę, możesz wykryć problem i chronić dzieci o wiele skuteczniej niż jakakolwiek technologia. Dodatkowe kroki:

* Dowiedz się, w jakie gry gra dziecko i upewnij się, że są one dla niego odpowiednie.
* Ogranicz ilość informacji udostępnianych przez Twoje dzieci w Internecie. Na przykład nigdy nie powinny udostępniać swojego hasła, wieku, numeru telefonu ani adresu zamieszkania.
* Rozważ umieszczenie ich komputera w miejscu, gdzie możesz mieć na nie oko. Ponadto młodsze dzieci nie powinny grać bez nadzoru rodzica lub opiekuna.
* Zastraszanie, wulgarny język lub inne aspołeczne zachowania mogą stanowić problem. Miej oko na swoje dzieci. Jeśli wydają się zdenerwowane, mogły zostać zastraszone w Internecie. Jeśli są prześladowane w Internecie, należy bezzwłocznie to zgłosić. Przypilnuj, żeby dzieci grały tylko z zaufanymi i odpowiednimi osobami.
* Dowiedz się, czy gra obsługuje zakupy w aplikacji i jakie są rodzaje kontroli rodzicielskiej.

****

**Redaktor gościnny**

Charlie Goldner jest założycielem CyberNV i instruktorem SANS. Aktywnie działa na LinkedIn i pracuje wspierając agencje rządowe. Przez lata spędził wiele godzin grając w gry komputerowe.

**Źródła**

**Ataki socjotechniczne:** <https://www.sans.org/newsletters/ouch/social-engineering-attacks/>

**Zabezpieczenie kont online:** <https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/>

**Menedżer haseł:** <https://www.sans.org/newsletters/ouch/password-managers/>

**Bezpieczeństwo dzieci online:** <https://www.sans.org/newsletters/ouch/online-security-kids/>

**Polski przekład CERT Polska:** Bartłomiej Wnuk, Aleksandra Węgrzynowicz

OUCH! jest publikowany przez firmę SANS Security Awareness i jest rozpowszechniany pod licencją[Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nd/4.0/legalcode). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszenia zawartości samego biuletynu. Zespół redaktorski: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.