Zagrożenia cyfrowej tożsamości dzieci i młodzieży w social mediach

3 czerwca 2022

webinar poprowadzi
Mariusz Stasiak vel Stasek

ISSA POLSKA

“Cyfrowy Skaut” - ISSA KIDS Awareness

Cele projektu

- Angażować specjalistów cyberbezpieczeństwa w edukację,
- Budować u rodziców świadomość zagrożeń w sieci,
- Chronić najmłodszych poprzez edukację,
- Dostarczać pomysły na lepsze wykorzystanie technologii,
- Edukować nauczycieli aby mogli dzielić się tą wiedzą w szkole.

Agenda

- Co to jest tożsamość cyfrowa?
- Gdzie posługujemy się naszą tożsamością cyfrową?
- Kto może chcieć nam ukraść naszą cyfrową tożsamość?
- Po co komu tożsamość cyfrowa dziecka lub nastolatka?
- Jak się bronić przed kradzieżą?
- Gdzie szukać pomocy?

Inspektor Ochrony Danych w
sektorze oświaty,
Auditor ISO 27001
wykładowca cybersecurity MBA

Co to jest tożsamość cyfrowa?

Cyfrowa tożsamość jest dość podobna do realnej. Zgodnie z definicją, zawiera zestaw danych, które w sposób jednoznaczny identyfikują osobę posługującą się tą **tożsamością**. Może zawierać dane i podpis wystawcy tejże **tożsamości**, co odgrywa rolę uwiarygodnienia informacji przez serwis internetowy lub oprogramowanie.

Gdzie posługujemy się naszą tożsamością cyfrową?

Gry, serwisy społecznościowe, fora internetowe, komunikatory oraz różne usługi cyfrowe – tożsamość cyfrowa stała się nieodłącznym elementem tych dziedzin naszego życia.

Zakładasz konto w Fortnite, Roblox czy Simsach?
Masz profil na Facebooku, TikTok'u czy Instagramie lub Snapchacie?
Komunikujesz się za pomocą Messengera, WhatsAppa czy Discorda, a może udzielasz się na forach internetowych?

We wszystkich tych miejscach posługujesz się swoją cyfrową tożsamością.

Kto może chcieć nam ukraść naszą cyfrową tożsamość?

Jeśli ktoś nie gra w gry online, to trudno mu wierzyć, że kradzież składającej się tylko z bitów i bajtów postaci z gry może być lukratywnym interesem.

Ale tak jest, bo sztuczne postaci mają realną wartość: chcąc wstąpić do wirtualnego świata World of Warcraft, musimy najpierw za 60 złotych nabyć grę, a potem odprowadzać do wiodącej na rynku gier online firmy Blizzard 45 złotych abonamentu miesięcznie. Każdy fan inwestuje w grę nie tylko pieniądze, ale także i czas: im dłużej gra, tym bardziej cenny staje się jego bohater, który nabiera tym samym realnej, przeliczalnej na pieniądze wartości.

Niektórzy gracze mają wprawdzie pieniądze, ale nie mają ochoty na długie rozwijanie umiejętności bohatera, więc popyt na doświadczone postaci jest duży, a gdzie jest popyt, tam znajdzie się i podaż - odpowiednie oferty możemy znaleźć na przykład na e-Bay'u. Postacie zmieniają właścicieli nawet za sumy rzędu 4000 złotych. Skradzionych postaci praktycznie nie można odróżnić od legalnych ofert.

https://www.komputerswiat.pl/poradniki/jak-to-dziala/jak-dzialaja-zlodzieje-kont-mmorpg/kx4mbx1

Po co komu tożsamość cyfrowa dziecka lub nastolatka?

Zdobyte doświadczenie, itemy czy skille mają wartość nie tylko w grze? Na różnych aukcjach czy forach internetowych użytkownicy sprzedają je za spore pieniądze, a co za tym idzie mają one realną wartość w prawdziwym świecie.

Konto w social media lub forach internetowych są wykorzystywane np. do serzenia nieprawdziwych informacji (fake news) czy do działań przestępczych (słupy).

Niestety często skradzione konto wykorzystywane jest również do szantażu czy prób wymuszeń.

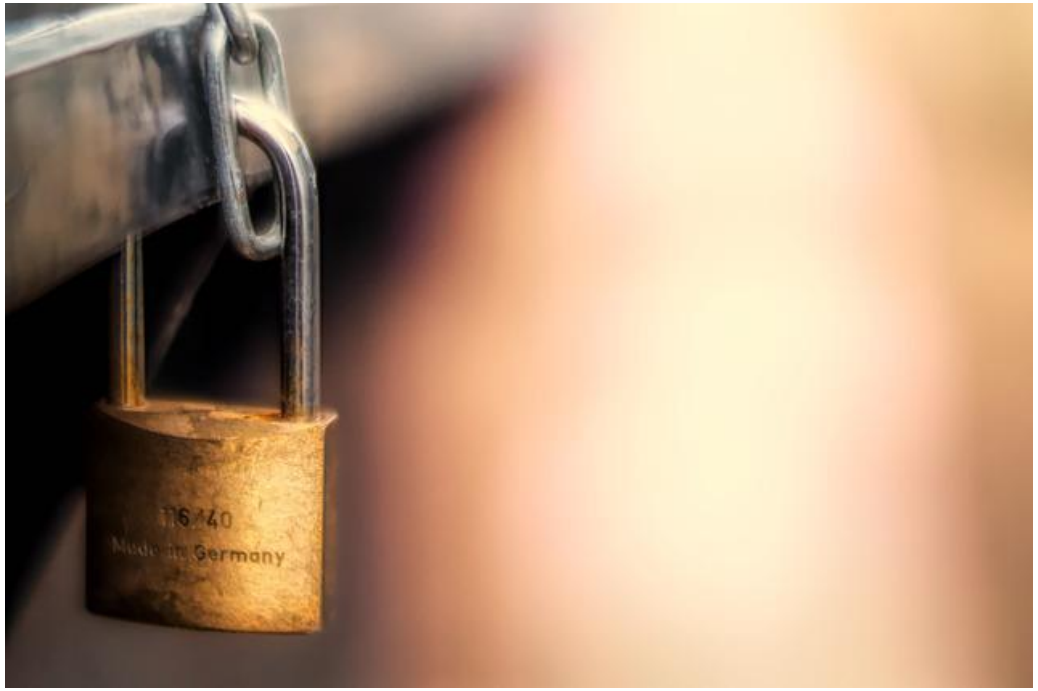
Do kont w grach bardzo często podpięte są również karty kredytowe np. rodziców co cyberoszuści z wielką przyjemnością wykorzystują.

Jak się bronić przed kradzieżą?

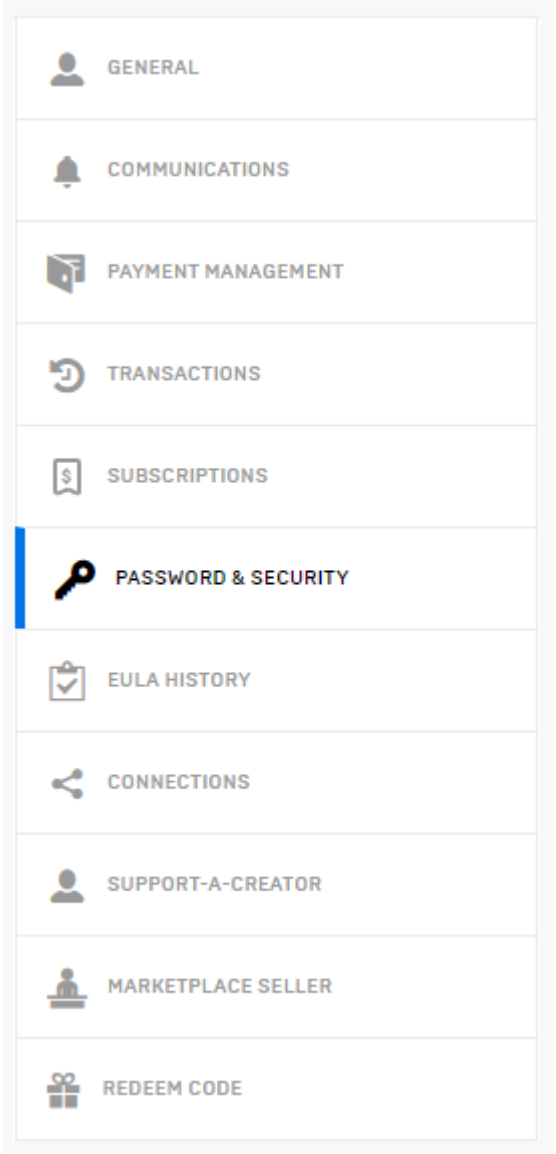
- Zmień hasło.
- Zweryfikuj swój adres e-mail.
- Włącz logowanie dwuetapowe (2EL) na swoim koncie.
- Zabezpiecz swoją skrzynkę e-mail u dostawcy usług poczty elektronicznej.
- Włącz opcję 2EL na wszystkich kontach powiązanych z Twoim kontem np. w serwisach Microsoft, Nintendo, Sony, Facebook lub Google.

Logowanie dwuetapowe i jak je włączyć

- https://www.epicgames.com/help/pl/konta-epic-c74/bezpieczenstwo-konta-c112/logowanie-dwuetapowe-i-jak-je-wlaczyc-a3218
- https://support.google.com/accounts/answer/185839?hl=pl&co=GENIE.Platform%3DDesktop
- https://support.microsoft.com/pl-pl/account-billing/w%C5%82%C4%85czenie-lub-wy%C5%82%C4%85czanie-weryfikacji-dwuetapowej-konta-microsoft-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca
- https://pl-pl.facebook.com/help/147926301947841



Epic Games



Konto Google

Włączanie weryfikacji dwuetapowej

Weryfikacja dwuetapowa (nazywana też uwierzytelnianiem dwuskładnikowym) dodatkowo zabezpiecza konto na wypadek kradzieży hasła. Po skonfigurowaniu weryfikacji dwuetapowej możesz logować się na swoje konto w dwóch etapach za pomocą:

- informacji, które znasz (na przykład hasła);
- czegoś, co masz (na przykład telefonu).

Włączanie weryfikacji dwuetapowej

1. Otwórz swoje konto Google.
2. W panelu użytkownika kliknij **Bezpieczeństwo**.
3. W sekcji „Logowanie się w Google” wybierz **Weryfikacja dwuetapowa** › **Rozpocznij**.
4. Postępuj zgodnie z instrukcjami na ekranie.

Twoje konto (nazwa_użytkownika@gmail.com) jest powiązane z Twoją firmą lub szkołą. Jeśli nie możesz skonfigurować weryfikacji dwuetapowej, skontaktuj się z administratorem.

Potwierdzanie swojej tożsamości za pomocą drugiego etapu

Po włączeniu weryfikacji dwuetapowej musisz przejść drugi etap logowania, by potwierdzić, że to Ty. Aby chronić Twoje konto, Google poprosi Cię o wykonanie określonej czynności na drugim etapie.

Facebook

Uwierzytelnianie dwuskładnikowe to funkcja zabezpieczeń, która pomaga chronić Twoje konto na Facebooku oraz hasło. Po skonfigurowaniu uwierzytelniania dwuskładnikowego wymagane jest wprowadzenie specjalnego kodu logowania lub potwierdzenie próby zalogowania za każdym razem, gdy ktoś spróbuje uzyskać dostęp do Facebooka z nieznanej przeglądarki lub nierozpoznanego urządzenia mobilnego. Powiadomienia możesz otrzymywać także za każdym razem, gdy ktoś spróbuje zalogować się z nieznanej przeglądarki lub nierozpoznanego urządzenia mobilnego.

Aby włączyć opcję uwierzytelniania dwuskładnikowego lub zarządzać nią:

1. Przejdź do menu Ustawienia bezpieczeństwa i logowania.
2. Przewiń w dół do opcji **Używaj uwierzytelniania dwuskładnikowego** i kliknij **Edytuj**.
3. Wybierz metodę zabezpieczającą, którą chcesz dodać, i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Podczas konfigurowania uwierzytelniania dwuskładnikowego na Facebooku pojawi się monit o wybranie jednej z trzech metod zabezpieczających:

- Dotknięcie klucza zabezpieczeń na kompatybilnym urządzeniu.
- Kody logowania z zewnętrznej aplikacji uwierzytelniającej.
- Wiadomości SMS z kodami w telefonie komórkowym.

Microsoft

Włączenie lub wyłączanie weryfikacji dwuetapowej konta Microsoft

Microsoft account, Pulpit nawigacyjny konta Microsoft

Za każdym razem, gdy będziesz logować się na urządzeniu, które nie jest zaufane, gdy włączona jest weryfikacja dwuetapowa, otrzymasz kod zabezpieczający za pośrednictwem poczty e-mail lub telefonu. Jeśli wyłączysz weryfikację dwuetapową, będziesz okresowo otrzymać i ponownie wysłać kody zabezpieczeń, wraz z każdym razem, gdy będzie to stanowić zagrożenie dla bezpieczeństwa Twojego konta. Jeśli nie chcesz używać poczty e-mail, połączenia telefonicznego ani wiadomości SMS, możesz za pomocą aplikacji Microsoft Authenticator ułatwić wzmacnianie zabezpieczeń konta i logowanie się bez haseł. Aby włączyć lub wyłączyć weryfikację dwuetapową:

1. Przejdź do ustawień zabezpieczeń i zaloguj się za pomocą konta Microsoft.

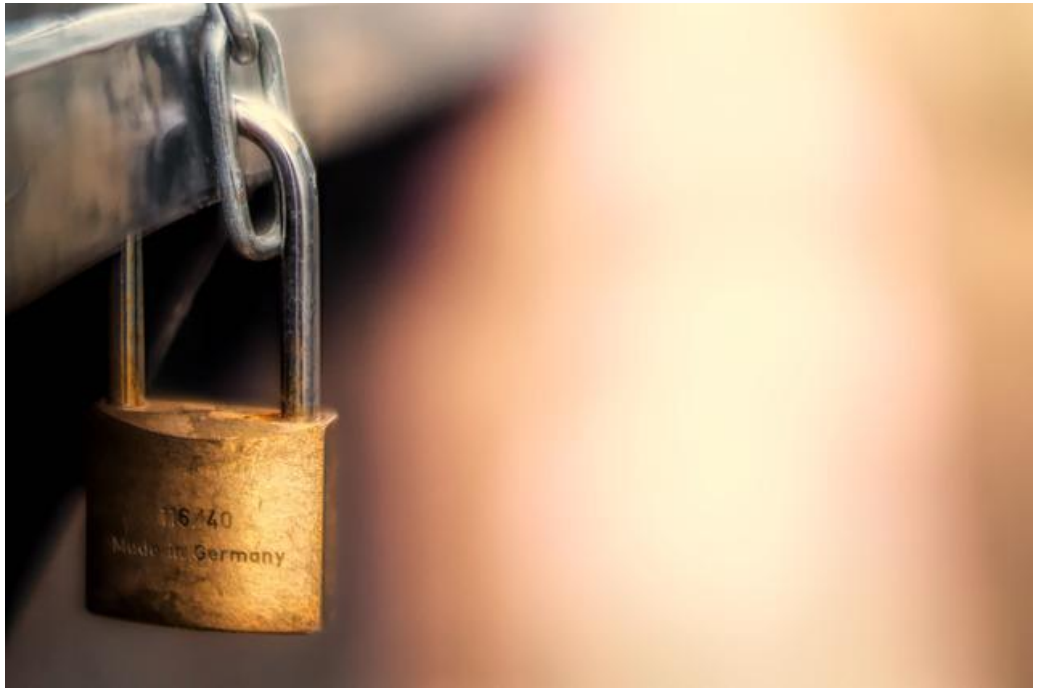
2. W sekcji **Weryfikacja dwuetapowa** wybierz pozycję Skonfiguruj weryfikację dwuetapową, aby ją włączyć, lub wybierz pozycję Wyłącz weryfikację dwuetapową, aby ją wyłączyć.

3. Postępuj zgodnie z instrukcjami.

Gdzie szukać pomocy?

Nie rozwiązuj problemu sam.

- Skontaktuj się z dostawcą usługi cyfrowej
- Poszukaj pomocy u rodziców i nauczycieli
- Skorzystaj z gotowych poradników (filmy i artykuły) jak odzyskać konto w danym serwisie
- Jeżeli podejrzewasz, że konto zostało wykorzystane w celach przestępczych skontaktuj się z policją
- Korzystaj z wiedzy i pomocy fachowców, którzy chętnie się nią dzielą na formach internetowych



https://www.moje-idealia.pl/2018/07/jak-zgosic-kradziez-konta-na-instagramie.html#

https://www.facebook.com/help/1216349518398524

https://www.epicgames.com/help/pl/konta-epic-c74/bezpieczenstwo-konta-c112/co-mam-zrobic-jesli-ktos-wlamie-sie-na-moje-konto-a3665

https://cyfrowyskaut.pl/