Cyberzagrożenia w świecie rzeczywistym

#phishing #scam
#inżynieria_społeczna

Cyberbezpieczeństwo

Cyberbezpieczeństwo jest to stan, w którym nie ma cyberzagrożeń. Niby proste i oczywiste, ale czy możliwa jest całkowita eliminacja czyhających w sieci niebezpieczeństw? Niestety cyberzagrożenia wynikają z czynników zewnętrznych, na które nie mamy wpływu. Możemy natomiast nauczyć się bezpiecznego poruszania w sieci i zwiększyć poziom ochrony, a tym podwyższyć naszą odporność na cyberzagrożenia.

Na cyberataki narażeni jesteśmy wszyscy, nie tylko duże firmy, które z racji swojej wielkości są łakomym kąskiem dla cyberprzestępców. Celem tzw. mikroataków są najczęściej osoby z mniejszą świadomością zagrożeń, a w szczególności dzieci.

Jakie są cyberzagrożenia?

Przede wszystkim – realne. Nakierowane na człowieka, wykorzystują nasze naturalne ludzkie odruchy – chęć pomocy, sympatię do drugiej osoby, podporządkowanie się autorytetom, niewiedzę czy po prostu zwykły pośpiech i wynikającą z niego nieuwagę.

Internetowi przestępcy mogą być specjalistami od budowania relacji i tworzenia personalizowanych treści nakierowanych na konkretną, wąską grupę ludzi. Mogą również działać na dużą skalę, wysyłając automatycznie maile do setek osób dziennie. Doskonale wiedzą, że zawsze znajdzie się odbiorca, któremu spreparowana treść wyda się na tyle wiarygodna, aby otworzyć załącznik czy podjąć próbę zalogowania się na zewnętrznym portalu. Załącznik będzie oczywiście zawierał wirusa, a portal będzie do złudzenia przypominał serwis internetowy, z którego na co dzień korzystamy.

Cyberprzestępcy działają każdego dnia i regularnie wprowadzają nowe formy cyberataków. Większość opiera się na inżynierii społecznej, czyli umiejętności manipulacji użytkownikami, by wyłudzić informacje, pieniądze lub skłonić do określonego działania.

Do najczęstszych cyberataków należą

- **Scamy**, czyli wyłudzenia pieniędzy.
- **Phishing** polegający na tym, że użytkownik ma kliknąć w link, który tak naprawdę jest wirusem lub oprogramowaniem szpiegującym (śledzącym to, co użytkownik robi za pomocą smartfonu). Fałszywe wiadomości mogą być rozsyłane mailowo (phishing) lub SMS-em (smishing). Natomiast vishing to próba wyłudzenia informacji podczas rozmowy telefonicznej.
- **Malvertising** – fałszywe reklamy darmowych aplikacji, które okazują się być wirusem.
- **Gry sieciowe** pochodzące z nieznanych źródeł mogą być ukrytymi programami szpiegującymi lub miejscem, w którym ukrywają się cyberprzestępcy.

Najczęstszym sposobem, którego chwytają się internetowi przestępcy, jest **oczekiwanie pilnego działania**. W ten sposób cyberprzestępcy wykorzystują nieuwagę, pośpiech, a niekiedy i naszą naiwność, zwłaszcza w połączeniu ze strachem. Nieopłacony rachunek? Paczka nie dojdzie, jeśli nie dopłacisz kilkudziesięciu groszy do przesyłki? Zostały ostatnie 3 sztuki tego świetnego telefonu po okazyjnej cenie? To są przykłady najpopularniejszych scenariuszy, do których przestępcy mają na pęczki.

Jak zadbać o cyberbezpieczeństwo dzieci?

Skoro my, dorośli, jesteśmy tak podatni na wyłudzenia, jak możemy uchronić nasze dzieci przed cyberprzestępcami czyhającymi w Internecie? **Zacznijmy przede wszystkim od siebie**. Zapoznajmy się chociaż w podstawowym zakresie z zasadami bezpiecznego przeglądania sieci, abyśmy mogli świadomie umożliwić dziecku korzystanie z zasobów sieci. Niemniej istotną kwestią będzie również wejście w świat naszego dziecka. Wiedza, z jakich serwisów, aplikacji i usług nasza pociecha korzysta na co dzień oraz jakich ludzi spotyka w świecie wirtualnym.

Nie jesteśmy w stanie całkowicie usunąć zagrożeń, ale możemy nauczyć dzieci, jak je rozpoznawać i się przed nimi chronić. Jak zatem zadbać o cyberbezpieczeństwo dzieci?

1. Zainstalować oprogramowanie do **kontroli rodzicielskiej**. Dzięki temu nie tylko rozeznamy się, z jakich serwisów korzystają nasze dzieci, ale również będziemy mieli względną kontrolę nad dostępem do tych treści. Pamiętajmy jednak, aby pilnować hasła czy PIN-u do tych aplikacji. Dzieci również potrafią wyłudzać poświadczenia od rodziców!
2. **Edukować dzieci**, że nie wszystko, co czytają i widzą w Internecie to prawda. Informacje, które znaleźliśmy w sieci, nie muszą być prawdziwe. Stronę internetową może założyć każdy. Edytować wpisy w encyklopedii internetowej – każdy. Publikować dowolne treści w social mediach – bez ograniczeń, byle były zgodne z ogólnym regulaminem danego serwisu.
3. Wytłumaczyć dzieciom **zasadę ograniczonego zaufania** do internetowych treści. Zasadę tę możemy uogólnić na wszystkie media, nie tylko cyfrowe. Wiadomości mogły zostać poddane manipulacji lub - wyrwane z kontekstu – dają zupełnie inny wydźwięk, niż pierwotnie zamierzony. Warto wspólnie przeglądać Internet i dyskutować z dzieckiem nad znalezionymi informacjami.
4. **Nauczyć dużej ostrożności w publikowaniu treści** o sobie czy o rodzinie. Skrawki informacji publikowane w social mediach są dla przestępców jak puzzle, z których mogą zbudować solidną podstawę do skopiowania naszej tożsamości lub przekonać, że jesteśmy celem wartym uwagi.
5. Uświadomić dzieciom, że podawanie **danych osobowych**, w tym domowego adresu czy szkoły, do której chodzą, może być niebezpieczne. Zwłaszcza w połączeniu z poprzednim punktem ujawnianie danych adresowych daje przestępcom przepustkę nie tylko do kradzieży tożsamości, ale i fizycznego ataku w realnym świecie.
6. Stosować **przedpłacone karty płatnicze** dla dzieci zamiast podpinania kart kredytowych do zakupów internetowych (zwłaszcza w grach). Będziemy mieli kontrolę nad wydatkami i spokój, że nie zaskoczy nas nagły brak środków na koncie.
7. Wprowadzić zasadę **różnych haseł do kont na stronach internetowych** czy mediach społecznościowych. W przypadku wycieku danych logowania z jednego portalu będziemy spokojni, że nikt nie zaloguje się tymi samymi poświadczeniami na innym serwisie, z którego korzystamy. Stosowanie tej reguły będzie dodatkowym środkiem ochronnym na wypadek ataku phishingowego, w którym nieświadomie my lub nasze dziecko podejmiemy próbę zalogowania się na fałszywym portalu.

Gdzie szukać pomocy?

Telefon zaufania dla dzieci i młodzieży to **116 111** lub **800 12 12 12**, czynny codziennie, 24 godziny na dobę. Strona internetowa: **116111.pl** – wystarczy się zarejestrować i skontaktować z konsultantami mającymi dyżur online.

Telefon dla rodziców, nauczycieli oraz opiekunów to **800 100 100**, czynny w dni powszednie w godzinach 12:00 – 15:00. Strona internetowa: **800100100.pl**.

Poradnia Dziecko w Sieci Fundacji Dajemy Dzieciom Siłę: tel. **+48 22 826 88 62**, ul. Przybyszewskiego 20/24, Warszawa, e-mail: **poradniadws@fdds.pl**.

Gdzie zgłosić przestępstwo internetowe?

Zgłoś incydent | CERT.PL

Policja 997

Dowiedz się więcej