**Informacja prasowa**

**Warszawa, 04.11.2024 r.**

**„Milioner z Afryki”, „Żołnierz z USA” – popularne oszustwa internetowe**

**Internet to nieskończona przestrzeń możliwości i wygody, ale również potencjalne pole pułapek. Z roku na rok rośnie liczba zagrożeń związanych z aktywnością online, od oszustw po wycieki danych. Jak możemy skutecznie chronić się przed cyberprzestępcami? Oto najważniejsze zasady, które warto wprowadzić w życie, by bezpiecznie korzystać z sieci.**

W czasach, gdy niemal każda sfera życia przenosi się do Internetu, świadomość zagrożeń w sieci jest kluczowa. Cyberprzestępcy nieustannie doskonalą swoje metody, wykorzystując luki w systemach zabezpieczeń oraz ludzkie emocje, takie jak strach czy chęć zysku. Na szczęście istnieje wiele sposobów, by zadbać o bezpieczeństwo w sieci – od podstawowych zasad higieny cyfrowej po bardziej zaawansowane techniki ochrony danych. – *Z pewnością każdy niejednokrotnie słyszał o dwóch popularnych oszustwach internetowych – mowa tutaj o „Milionerze z Afryki” i „Żołnierzu z USA”. Mimo iż Internet to fantastyczne możliwości komunikacji, globalnego połączenia ze światem oraz furtka do niezliczonych osiągnięć, tak też niestety jest drzwiami do nieuczciwych działań, w tym rozwijających się nieustannie oszustw internetowych –* mówi **Marta Fila, członek zarządu AIQLabs, właściciela marek SuperGrosz i „Kupuj Teraz – zapłać później”.**

Tworzenie silnych haseł to jeden z najprostszych, ale i najważniejszych kroków w kierunku zabezpieczenia swoich danych. Niestety, wielu użytkowników Internetu nadal używa prostych, łatwych do odgadnięcia haseł, takich jak „123456” czy „password”. Aby zwiększyć poziom bezpieczeństwa, warto stosować unikalne kombinacje składające się z liter, cyfr i znaków specjalnych. Takie hasła są również coraz częściej wymagane przez strony www, także w momencie zakładania konta w sklepie internetowym. Dobrym rozwiązaniem jest również używanie menedżera haseł, który nie tylko wygeneruje skomplikowane hasło, ale także będzie je bezpiecznie przechowywał. Pamiętajmy również o regularnej zmianie haseł, zwłaszcza w przypadku najważniejszych kont, takich jak bankowe czy e-mailowe.

**Ostrożność w kontaktach online**

Niezwykle istotnym aspektem cyberbezpieczeństwa jest zachowanie ostrożności w kontaktach online. Oszuści coraz częściej podszywają się pod znane instytucje lub osoby, próbując wyłudzić pieniądze lub dane osobowe. Dwa popularne oszustwa internetowe – „Milioner z Afryki” i „Żołnierz z USA” – bazują na manipulacji emocjami, oferując szybki zysk lub apelując do patriotycznych uczuć ofiar. Mechanizmy te wykorzystują naszą łatwowierność, dlatego ważne jest, aby zawsze weryfikować tożsamość osób, z którymi się kontaktujemy, zwłaszcza jeśli nagle proszą nas o pieniądze lub poufne informacje. Zdrowy rozsądek i sceptycyzm są naszymi najlepszymi sojusznikami w walce z cyberoszustami. Jednym z najskuteczniejszych sposobów ochrony swoich kont internetowych jest włączenie tzw. dwustopniowego uwierzytelniania (2FA). Ta metoda wymaga nie tylko podania hasła, ale również dodatkowego potwierdzenia tożsamości, np. poprzez kod SMS lub aplikację uwierzytelniającą. Nawet jeśli ktoś zdobędzie nasze hasło, nie będzie mógł uzyskać dostępu do konta bez tego drugiego etapu weryfikacji. Warto korzystać z tej opcji, zwłaszcza w przypadku kont o wysokim stopniu wrażliwości, jak np. bankowość online.

**Regularne aktualizacje**

Posiadanie zaktualizowanego oprogramowania antywirusowego to absolutna podstawa każdego komputera i urządzenia mobilnego. Nowoczesne antywirusy oferują szereg dodatkowych funkcji, takich jak ochrona przed phishingiem (podszywaniem się pod wiarygodne strony) czy monitoring podejrzanych działań. Ważne jest także, aby regularnie aktualizować wszystkie systemy operacyjne oraz aplikacje. Twórcy oprogramowania stale pracują nad eliminacją luk w zabezpieczeniach, które mogłyby zostać wykorzystane przez hakerów, dlatego ignorowanie aktualizacji to otwarte zaproszenie do kłopotów.

Wielu użytkowników pada ofiarą cyberprzestępców, klikając na podejrzane linki lub otwierając załączniki w e-mailach od nieznanych nadawców. To jedna z najstarszych, ale wciąż najskuteczniejszych metod wyłudzania danych i instalowania złośliwego oprogramowania. Zasada jest prosta – nie klikajmy na linki ani nie otwierajmy plików, jeśli nie mamy pewności co do ich pochodzenia. Warto również nauczyć się rozpoznawać tzw. phishingowe wiadomości, które podszywają się pod znane instytucje, próbując nakłonić nas do podania danych logowania. Jeśli otrzymujemy e-mail z prośbą o zmianę hasła czy inne działania, zawsze warto najpierw skontaktować się bezpośrednio z daną firmą, korzystając z oficjalnych kanałów komunikacji.

Ostatecznie, kluczem do bezpieczeństwa online jest ciągła edukacja. Świat cyberzagrożeń dynamicznie się zmienia, a cyberprzestępcy opracowują coraz bardziej zaawansowane techniki. Regularne śledzenie informacji na temat nowych zagrożeń i metod obrony pozwala na lepsze przygotowanie się do potencjalnych ataków. Warto także uczestniczyć w szkoleniach z zakresu cyberbezpieczeństwa, które oferują firmy i instytucje publiczne. Im większą wiedzę posiadamy na temat zagrożeń, tym mniejsze jest ryzyko, że staniemy się ofiarą cyberprzestępstwa.

**\*\*\***

**AIQLABS Sp. z o.o. – zaawansowany FinTech od 2015 r. działający w branży consumer finance**. Misją firmy jest dostarczanie produktów finansowych dopasowanych do zdolności kredytowej i potrzeb klientów, dzięki zaawansowanej analityce, technologii i nowoczesnym procesom obsługi. Spółka oferuje kompletny ekosystem usług związanych z finansowaniem gotówkowym potrzeb zakupowych klientów, w tym kredyty konsumenckie, finansowanie usług medycznych oraz odroczone płatności za zakupy.

**Więcej informacji:**

[**http://aiqlabs.pl/**](http://aiqlabs.pl/)

[**https://kupujteraz.pl/**](https://kupujteraz.pl/)

[**https://supergrosz.pl/**](https://supergrosz.pl/)

**Kontakt dla mediów:**

**Bartosz Sosnówka**

communications manager

E: [Bartosz.sosnowka@dwapiar.pl](mailto:Bartosz.sosnowka@dwapiar.pl)

M: 517 476 361