**Informacja prasowa**

**Warszawa, 04.03.2024 r.**

**Realne zagrożenie dla danych i urządzeń. Rozpoznawanie niechcianego maila**

**Cyberbezpieczeństwo to obecnie priorytet w każdej organizacji, działającej w Internecie czy chmurze. Odpowiednia ochrona jest kluczem do uniknięcia ataków i innych zagrożeń, przed którymi stoją firmy. Z badania SonicWall, dotyczącego największych zagrożeń, z jakimi mierzą się przedsiębiorstwa, aż 66% ankietowanych wskazało zagrożenia cyberatakami. Raport pokazał, że w sieci nikt nie jest bezpieczny, jednak wirtualnych ataków można się ustrzec.**

Złośliwe lub zaszyfrowane oprogramowanie to aplikacja, której celem jest spowodowanie uszkodzenia systemów, kradzież danych, uzyskanie nieautoryzowanego dostępu do sieci lub sianie spustoszenia w inny sposób. Jest to najczęstszy rodzaj cyberzagrożenia. Według badania SonicWall, złośliwe oprogramowanie zajęło trzecie miejsce, jeśli chodzi o obawy respondentów co do sposobu ataku. Aż 76% respondentów obawia się także ataków phishingowych. Wyłudzanie informacji to powszechna technika ataku, która manipuluje ludźmi w celu podjęcia niebezpiecznych działań lub ujawnienia poufnych informacji.

Poczta elektroniczna to obecnie nieodzowne narzędzie komunikacji zarówno w sferze osobistej, jak i zawodowej. Wraz z wykorzystaniem tej wygodnej formy kontaktu, narasta zagrożenie niechcianego maila, który może mieć szkodliwe skutki dla bezpieczeństwa i prywatności. Niezliczone wiadomości spamowe, podejrzane propozycje i niebezpieczne linki mogą stanowić realne zagrożenie dla naszych danych oraz urządzeń. Ważnym aspektem w walce z niechcianym mailem jest zdolność rozróżnienia bezpiecznego od podejrzanego linku.

*Phishingowe maile to nic innego jak oszustwa polegające na podszywaniu się pod rzeczywiste instytucje, takie jak banki, serwisy społecznościowe i tym podobne, w celu wyłudzenia poufnych informacji. Jeśli nadawca prosi o zaktualizowanie hasła lub inne dane, należy zalogować się bezpośrednio na oficjalnej stronie, a nie poprzez link w mailu. Przejeżdżając kursorem myszy nad linkiem, należy także zwrócić uwagę na adres URL, który pojawia się w dolnym rogu przeglądarki. Chodzi o upewnienie się, że adres wygląda wiarygodnie i odpowiada temu, co sugeruje treść wiadomość. Jeśli nadesłany link prowadzi do strony internetowej, której nie rozpoznajemy lub której zaufanie budzi wątpliwości, lepiej powstrzymać się od kliknięcia. Należy też unikać klikania w skrócone linki, które mogą prowadzić do nieznanych witryn –* mówi **Marta Fila, członek zarządu w AIQLabs, właścicielu marek SuperGrosz i „Kupuj Teraz – zapłać później”.**

Niechciany mail stanowi poważne zagrożenie dla bezpieczeństwa online. Głównym celem cyberprzestępców są zwykle najwrażliwsze dane każdego z nas, czyli hasła, poufne dane czy finanse. Kluczowym elementem w zachowaniu ochrony jest odróżnianie potencjalnie szkodliwych od bezpiecznych linków. Należy zawsze zachować czujność, ponieważ dbanie o bezpieczeństwo własnej skrzynki odbiorczej to podstawowy krok, który warto podjąć, aby uniknąć niechcianych maili i możliwych cyberataków.

**\*\*\***

**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

M: 517 476 361