**Informacja prasowa**

**Warszawa, 05.09.2024 r.**

**Wysyłanie dokumentów drogą mailową**

***Kluczowe aspekty związane z bezpieczeństwem online***

**Wysyłanie dokumentów mailem stało się naturalnym procesem w czasach rozwijającej się cyfryzacji oraz rosnącej roli Internetu, który jest niezbędnym narzędziem do pracy i rozrywki. To szybkie, wygodne i efektywne narzędzie, umożliwiające udostępnianie informacji zaledwie kilkoma kliknięciami. Za tym ułatwieniem kryją się jednak pewne istotne aspekty dotyczące bezpieczeństwa, które nie powinny być bagatelizowane.**

Mimo zaawansowanych technologii, to błąd ludzi nadal jest jednym z największych zagrożeń, jakie mogą spotkać nas w trakcie wysyłania dokumentów drogą mailową. Korespondencja skierowana do niewłaściwego adresata lub przypadkowe ujawnienie poufnych danych może prowadzić do poważnych konsekwencji. Należy również pamiętać, że osoby trzecie mogą wykorzystać oszukańcze metody, jak na przykład phishing, aby zdobyć poufne dane, czyli hasła dostępu do dokumentów lub konta mailowego.

**Łatwy cel dla cyberprzestępców**

Wysyłając dokumenty, istnieje ryzyko, że odbiorca może zostać oszukany lub zaatakowany. Niezabezpieczony mail może stać się także łatwym celem dla cyberprzestępców, którzy mogą przechwycić wiadomość i uzyskać dostęp do zawartości dokumentów. To z kolei może prowadzić do naruszenia prywatności oraz wycieku poufnych informacji.

*Wysyłanie dokumentów mailem może być bezpieczne, jeśli stosujemy odpowiednie środki ostrożności. Dwuetapowa weryfikacja, ochrona przed złośliwym oprogramowaniem, silne hasła, a także szyfrowanie, to tylko niektóre z kluczowych elementów, które warto wziąć pod uwagę. Pamiętajmy, że dbanie o bezpieczeństwo informacji jest wspólnym wysiłkiem nadawców i odbiorców. W związku z tym, warto zastanowić się, czy zastosowane środki ochrony są wystarczające, aby zapewnić poufność i integralność naszych danych* – mówi **Marta Fila, członek zarządu AIQLabs, właściciela marek SuperGrosz i „Kupuj Teraz – zapłać później”.**

**Sposoby ochrony przed cyberatakiem**

Włączenie dwuetapowej weryfikacji dla konta mailowego zwiększa bezpieczeństwo poprzez dodatkową warstwę ochrony przy logowaniu. Aktualne oprogramowanie antywirusowe minimalizuje z kolei ryzyko przechwycenia danych przez złośliwe oprogramowanie. Ponadto, zarówno nadawca, jak i odbiorca dokumentów powinni korzystać z silnych, unikalnych haseł do swoich kont mailowych. Zmniejsza to ryzyko nieautoryzowanego dostępu.

Wykorzystywanie szyfrowania end-to-end jest kluczowe dla ochrony dokumentów. Szyfrowanie pozwala na zakodowanie treści wiadomości w taki sposób, że tylko zamierzony odbiorca będzie w stanie ją odczytać. Wysyłając ważne dokumenty, warto także unikać korzystania z publicznych sieci Wi-Fi, które mogą być narażone na przechwycenie danych. Ostatecznie, bezpieczeństwo przesyłania dokumentów zależy od zastosowania właściwych praktyk zabezpieczających poufne informacje.

**\*\*\***

**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