

AKCJA PHISHINGOWA Z WYKORZYSTANIEM MARKI POCZTY POLSKIEJ. OSZUŚCI NIE ODPUSZCZAJĄ

Cyberprzestępcy ponownie próbują wyłudzić dane wrażliwe lub informacje poufne, podszywając się pod Poczta Polska - alarmuje Spółka, wskazując na konieczność zachowania szczególnej uwagi i ograniczonego zaufania do roszczeń otrzymywanych w e-mailach lub na odwiedzanych stronach internetowych.

„Ryzyko akcji phishingowych wzrasta. Cyberprzestępcy coraz częściej próbują wyłudzić dane wrażliwe internautów, aby następnie wykorzystać je w nieuczciwych celach. Ataki phishingowe godzą nie tylko w dobre imię i interesy znanych oraz szanowanych firm, ale także w osoby prywatne, które często padają ofiarą oszustwa. Jednym ze sposobów przywłaszczenia danych osobowych internautów i ich kont jest wykorzystanie techniki manipulacji, polegającej na wywieraniu określonego wpływu i zachowania poprzez rozsyłanie wiadomości e-mail, z wykorzystaniem bardzo podobnych do oryginalnych i zastrzeżonych domen firm oraz instytucji” - tłumaczy Poczta Polska. Jak dodaje, największym zagrożeniem w takich sytuacjach bywa przekazanie przez internautę-adresata phishingowej wiadomości, dostępu do indywidualnego konta bankowości elektronicznej, danych logowania i wrażliwych danych osobowych.

W ramach najnowszej kampanii cyberprzestępcy ponownie podszywają się pod markę Poczty Polskiej, kierując do jej Klientów wiadomości phishingowe, w których nakłaniają do kliknięcia w podejrzany link – podobny do prawdziwej witryny Spółki. Podczas cyberataków wykorzystywany jest adres strony poczta-po1ska.pl, który różni się od prawdziwej tylko jednym znakiem – tj. cyfrą 1 zamiast podobnej do niej litery l.

Poczta Polska wskazuje na przykłady stron „www” nienależących do Spółki:

- **poczta-po1ska.pl (uwaga: cyfra „1” zamiast litery „l”)**
- poczta-polska[.pl (uwaga!!! wielka litera „i” zamiast malej litery „L”);
- pocztapolska[.]ga;
- pocztapolska[.]cf;
- polska-poczta[.]top;
- pomoc-poczta24[.]pl;
- poczta-polityka[.]net[.]pl;
- emonitoring-epoczta-polska[.]net;
- emonitoring-plpocztapolska[.]com;
- emonitoring-paypocztapolska[.]net;
- emonitoring-epocztapolska[.]com;
- tpocztapolska[.]com;
- platnosc8512-pocztapolska[.]net;
- monitoring-epocztapolska[.]net;
- eupocztapolska[.]com;

- emonitoring-upoczta.polska[.]net;
- emonitoring-epoczta.polska[.]net.

Aby nie paść ofiarą cyberprzestępców, ochronić swoje dane i majątek, Poczta Polska wskazuje na konieczność stosowania kilku podstawowych zasad:

1. uważnie czytaj adresy stron przesyłanych zarówno w mailach jak i SMS'em;
2. nie klikaj w odnośniki otrzymane od nieznanych nadawców;
3. nigdy nie odpowiadaj na żądania podania danych personalnych, haseł i/lub loginów do kont;
4. uważaj na błędy w treściach odnośników (np. zamieniona kolejność liter lub podstawienie innych liter, cyfr), jeśli takie znajdziesz, prawdopodobnie jest to oszustwo;
5. niektóre linki dołączone do wiadomości od nieznanych nadawców mogą instalować niechciane złośliwe oprogramowanie;
6. używaj oprogramowania antywirusowego, sprawdzaj jego aktualność i instaluj aktualizację oraz skanuj regularnie komputer;
7. regularnie zmieniaj hasła i dbaj o ich odpowiednią „siłę” nie używając haseł typu: 12345, QWERTY, imię, data urodzenia, Wiosna2021.

„W przypadku otrzymania podejrzanego e-maila lub w przypadku podejrzenia nieprawidłowości bądź niezgodności prosimy o niezwłoczne informowanie o zdarzeniu na adres email: cyberbezpieczenstwo@poczta-polska.pl” - wskazuje Poczta Polska.

Informacja prasowa Poczty Polskiej

Czytaj też: [Marka Poczty Polskiej jest atrakcyjna dla cyberprzestępców](#)