CyberŚwięta w Banku BPS
SOC BPS ostrzega!

W okresie przedświątecznym cyberprzestępcy wykorzystują gorączkę zakupów i dezinformację, aby nakłonić użytkowników do podjęcia nieprzemyślanych działań. W Raporcie rocznym CSIRT KNF na rok 2024 potwierdzono, że widoczna jest sezonowość **ataków** i odnotowuje się „**znaczny wzrost aktywności** w czasie intensywnych zakupów online, takich jak Black Friday, Cyber Monday oraz **przed świętami**".

Najpopularniejsze przykłady phishingu

- Podszycie pod dział HR/zarząd firmy z informacją o premiach lub bonie świątecznym
- Podszycie pod znane firmy kurierskie (jak InPost, DPD, DHL, Poczta Polska
- Podszycie pod popularne platformy zakupowe np. Allegro, Amazon Zalando
- Oszustwa związane z płatnościami online i bankowością – fałszywe strony pośredników
- Fałszywe oferty sprzedaży na social-media
- Fałszywe zbiórki charytatywne

Ataki **skierowane do pracowników** – cyberprzestępcy **podszywają się pod dział HR** i przesyłają maile z prośbą o wypełnienie formularza w celu odebrania **rzekomej premii lub nagrody świątecznej**

Ataki wykorzystujące schemat z **„Dopłatą do paczki", „Paczka zatrzymana w urzędzie celnym"** czy **„Zmień termin dostawy"**

Cyberprzestępcy tworzą strony internetowe do **złudzenia przypominające popularne sklepy** lub witryny znanych marek, oferując przy tym niesamowite, **"świąteczne" promocje**. Strony wyglądają wiarygodnie, ale mają drobne błędy w adresie URL np. zalando-poland.pl zamiast zalando.pl

Cyberprzestępcy tworzą **fałszywe strony pośredników płatności** (jak PayU, Przelewy24), na które kierują ofiary po kliknięciu w link rzekomo w celu opłacenia zakupów, wyłudzając dane do logowania do bankowości elektronicznej

Ataki z **wykorzystaniem reklam sponsorowanych** na m.in. Facebooku czy Instagramie, promujące luksusowe produkty (np. elektronikę, markowe ubrania) w szokująco niskich cenach. Kliknięcie prowadzi do fałszywej strony wyłudzającej m.in. dane finansowe.

Cyberoszuści tworzą **zmyślone zbiórki na cele charytatywne** i zachęcają do wpłat za pomocą linków do fałszywych stron płatności.

Zawsze weryfikuj nadawcę.

Nigdy nie klikaj w podejrzane linki.

Używaj silnych haseł i włącz uwierzytelnianie dwuskładnikowe (2FA)

Pamiętaj ! Otwierając "kartkę świąteczną" lub "list od Mikołaja" w załączniku możesz nieświadomie zainstalować złośliwe oprogramowanie

Nie daj się oszukać cyberprzestępcom!
Niech jedyny KTO Cię zaskoczy to Święty Mikołaj z prezentami pod choinką!

SOC Zrzeszeni w bezpieczeństwie