SEKURAK.PL

[PHISHING]

[HACKING DETECTED.....]

PHISHING E-MAIL

Czym grozi skuteczny phishing?

- Kradzież poufnych danych
- Kradzież pieniędzy
- Infekcja komputera
- Zablokowanie infrastruktury IT oraz straty operacyjne
- Straty reputacyjne

Rozpoznawanie phishingu

- Jeśli nie masz pewności, czy e-mail jest prawdziwy, zadzwoń do nadawcy (banku, urzędu, prezesa, ...)
  - Wybierz numer ręcznie, nie dzwoń na numer podany w e-mailu
- Weryfikuj adres e-mail nadawcy (nie jego nazwę)
  - Uwaga również na wiadomości pochodzące od zaufanego nadawcy
    - Zhackowana skrzynka
    - Podszywanie się pod dowolny adres e-mail
    - Tricki umożliwiające atakującym wysyłanie e-maili z prawdziwych serwisów
- Zastanów się, jakie emocje wywołuje
  - Strach / presja czasu
    - „Zhackowano konto”
    - Pilna prośba od prezesa
    - „Zawieszamy Twoje konto”
    - „Naruszyłeś prawa autorskie”
  - Chęć zysku
    - „Wygrałeś iPhone’a!”
    - „Laptopy dla pracowników z 90% rabatu!”
  - Ciekawość
    - „Zobacz, ile zarabia zarząd”
  - Autorytet
    - Prezes: „proszę pilnie wysłać ten przelew”
    - Osobista prośba od prezesa: Prokuratura: „proszę pilnie przelać pieniądze!”
  - Pośpiech / rutyna
    - „Dopłać do paczki”
- Phishing nie zawsze zawiera błędy językowe
- Czy e-mail zawiera linki / załączniki?

Co warto wiedzieć o linkach?

- Linki-skracacze
  - Nazwa linku i adres linku to dwa różne pojęcia
  - Stosowane są w celu ukrycia podejrzanego adresu linku
  - Przykład: tinyurl.com/4eznc353
- Samo kliknięcie w link najczęściej nie infekuje komputera
  - Nie podawaj poufnych danych (np. haseł / danych osobowych) na nieznanych stronach
- Częste tricki w nazewnictwie linków
  - Celowo dodana jedna litera: np. sekuurak.pl
  - Nietypowa domena (np. sekurak.eu zamiast sekurak.pl)
  - twojbank.pl.sekurak.pl
  - Dziwne litery w nazwie, np.: https://sekurak.pl/

Co warto wiedzieć o załącznikach?

- Jak rozpoznawać złośliwe załączniki?
  - Sprawdzaj typ załącznika (kolumna Typ w Eksploratorze Windows)
  - Załącznik możesz wysłać do serwisu virustotal.com
    - Uwaga: nie wysyłaj tam poufnych danych!
- Samo zapisanie załącznika na dysku nie infekuje komputera
  - Infekcja może nastąpić dopiero po jego otwarciu
    - Antywirusy nie są idealne, mogą nie wykryć niektórych złośliwych plików
- Plik może być załączony bezpośrednio w e-mailu lub jako zewnętrzny link

Inne źródła phishingu

- SMS
- Rozmowa telefoniczna
- Kody QR
- Komunikatory
- Reklamy w Internecie

Jak reagować?

- Wyślij podejrzany e-mail do działu bezpieczeństwa / IT
  - Pamiętaj, żeby w treści napisać jedno zdanie – „Uwaga, to może być próba oszustwa"
- Otworzyłeś załącznik z e-maila?
  - Skontaktuj się pilnie z działem bezpieczeństwa / IT
- Podałeś poufne dane w linku z e-maila lub wysłałeś poufne dane, odpowiadając na e-mail
  - Skontaktuj się pilnie z działem bezpieczeństwa / IT
- Nie kontaktuj się z nadawcą phishingu!