cyber_Folks

checklista

>Phishing – co zrobić, kiedy dojdzie do ataku?_

wstępna diagnoza:

- [ ] Próba oszacowania, czy doszło do wykradzenia danych.
- [ ] Uzyskanie próbki wiadomości i ustalenie, jak ją odróżnić od prawdziwej.
- [ ] Sprawdzenie strony docelowej i ustalenie, jak ją odróżnić od prawdziwej.

zwróć uwagę na te elementy maila:

- [ ] nazwa nadawcy oraz ewentualne literówki
- [ ] adres e-mail nadawcy, a zwłaszcza domena
- [ ] temat – czy wygląda tak, jak na Twojej stronie?
- [ ] preheader
- [ ] szablon graficzny
- [ ] logo
- [ ] kolorystyka
- [ ] kroje pisma
- [ ] poprawność językowa
- [ ] styl wypowiedzi (kolokwializmy, dziwne sformułowania)
- [ ] poprawność stopki (czy jest w 100% zgodna z Twoją?).

zwróć uwagę na te elementy na stronie:

- [ ] domena widoczna w pasku przeglądarki (czyli część adresu zaraz po https:///),
- [ ] czy adres jest poprzedzony kłódką? (połączenie https://),
- [ ] jaki typ certyfikatu zainstalowano, czy jest taki sam jak na Twojej stronie?
- [ ] Logo, kolorystyka, kroje pisma, poprawność językowa
- [ ] Dane w stopce strony
- [ ] pokaż szczegóły certyfikatu – prawie na pewno będzie tam napisane R3 / Let's Encrypt. Zakładam, że Ty posiadasz SSL w walidacji EV, więc w Twoich informacjach o certyfikacie będzie nazwa Twojej Firmy. Na stronie fałszywej jej nie ma.