Temat: Bezpieczeństwo w Sieci – Phishing

Czym dokładnie jest phishing?

Phishing to jedna z najstarszych i najskuteczniejszych metod oszustwa w Internecie. Polega na podszywaniu się pod zaufane osoby lub instytucje (banki, firmy kurierskie, urzędy), aby wyłudzić od Ciebie poufne informacje: hasła, numery kart kredytowych czy dane osobowe.

Rodzaje pułapek, na które musisz uważać

Oszuści nieustannie modyfikują swoje metody. Najczęstsze z nich to:

- **E-mail phishing:** Wiadomości udające faktury, powiadomienia o blokadzie konta lub przesyłkach.
- **Smishing(SMS):**Krótkie wiadomości z linkiem do dopłaty za prąd lub paczkę (często kwoty rzędu 1-2 zł).
- **Vishing:** Rozmowy telefoniczne, w których oszust udaje pracownika banku, informując o rzekomym zagrożeniu Twoich oszczędności.

Anatomia ataku – Czerwone Flagi

Zanim klikniesz w jakikolwiek link, sprawdź, czy wiadomość zawiera te elementy:

- **Presja czasu i strach:** ”Twoje konto zostanie usunięte w ciągu 2 godzin!”, ”Działaj natychmiast!”.
- **Błędy i brak profesjonalizmu:** Błędy ortograficzne, dziwna składnia (często wynik tłumaczenia maszynowego), brak polskich znaków.
- **Podejrzany adres nadawcy:** Adres e-mail może wyglądać podobnie do prawdziwego (np. *kontakt@bnak.pl* zamiast *kontakt@bank.pl*).
- **Prośba o dane wrażliwe:** Pamiętaj, że banki nigdy nie proszą o podanie hasła przez email

Twoja tarcza obronna – Jak reagować?

Złote Zasady Bezpieczeństwa

1. **Nie klikaj w linki z nieznanych źródeł.** Zamiast tego wejdź na stronę banku, wpisując adres ręcznie w przeglądarce.
2. **Sprawdzaj certyfikat bezpieczeństwa.** Kliknij w ikonę kłódki przy adresie strony i sprawdź, dla kogo został wystawiony.
3. **Stosujzasadęograniczonegozaufania.** Jeśli "konsultant" prosi Cię o instalację aplikacji do zdalnego pulpitu (np. AnyDesk) – rozłącz się natychmiast!
4. **Weryfikuj dwuetapowo (2FA).** To najlepsza ochrona. Nawet jeśli oszust pozna Twoje hasło, nie wejdzie na konto bez kodu z Twojego telefonu.

Co zrobić, gdy padniesz ofiarą oszustwa?

Jeśli podałeś dane lub przelałeś pieniądze:

- Natychmiast zadzwoń na oficjalną infolinię swojego banku i zablokuj karty oraz dostęp do konta.
- Zmień hasła we wszystkich innych serwisach, w których używałeś tego samego hasła.
- Zgłoś sprawę na policję oraz do zespołu CERT Polska (na stronie incydent.cert.pl).