

CYBERBEZPIECZEŃSTWO FINANSOWE



TWORZENIE SILNYCH HASEŁ



BEZPIECZNY SKŁEP INTERNETOWY



PHISHING

Phishing to sytuacja, w której ktoś udaje kogoś innego w internecie, żeby wyłudzić informacje – na przykład hasło, numer telefonu albo zdjęcia. Taka osoba często próbuje cię oszukać, wysyłając fałszywe wiadomości, linki lub prośby, które wyglądają jak prawdziwe, ale mają cię wciągnąć w pułapkę. To “złapanie kogoś na haczyk” w internecie!

SILNE HASŁO = SILNA OCHRONA

- ▶ Mieszanka liter, cyfr i symboli
- ▶ Minimum 12 znaków
- ▶ Bez imienia, daty urodzenia, nazwy szkoły
- ▶ Każde konto = inne hasło
- ▶ Używaj menedżera haseł
- ▶ Nie zapisuj haseł w widocznym miejscu i nie dziel się hasłem z nikim poza rodzicem lub opiekunem

OPOWIEDZ HISTORIĘ, ŻEBY ZAPAMIĘTAĆ HASŁO

- ▶ Stwórz hasło z 2-3 losowych wyrazów + cyfry + znak specjalny.
- ▶ Wymyśl historię, żeby zapamiętać hasło.

PRZYKŁAD:

Hasło: KotDrzewo14!
Historia: Kot wspiał się na drzewo o 14!

PO CZYM POZNAĆ CZY NASZE ZAKUPY SĄ BEZPIECZNE W SIECI?

- ▶ Adres zaczyna się od „https:” – kłódka przy adresie strony oznacza, że link jest bezpieczny.
- ▶ Pozytywne opinie.
- ▶ Realne ceny – jeśli coś jest „za dobre, żeby było prawdziwe”, to zwykle jest oszustwem.
- ▶ Pełne dane firmy (e-mail, telefon, adres).
- ▶ Regulamin (dostępna polityka zwrotów i reklamacji).
- ▶ Płatność tylko przez zaufane systemy.

CIEKAWOSTKI

- ▶ Najpopularniejsze hasło na świecie to „123456”. I łamie się je w mniej niż sekundę.
- ▶ Hasło 12 znakowe może być milion razy bezpieczniejsze niż 6 znakowe.

CIEKAWOSTKI

- ▶ Adres fałszywego sklepu może tylko nieznacznie różnić się od prawdziwego – jedną literką, kropką lub kolejnością wyrazów.
- ▶ Co trzeci fałszywy sklep znika z internetu w mniej niż 48 godzin – zanim ktokolwiek zdąży zgłosić oszustwo.

NA CO UWAŻAĆ?

- ▶ **Obietnice nagród:** „Wygrałeś tablet, kliknij tutaj!”
- ▶ **Straszenie:** „Masz tylko 5 minut, żeby podać hasło! Inaczej twoje konto zostanie zablokowane!”
- ▶ **Prośby o dane:** „Podaj login i hasło, żeby odebrać prezent”.
- ▶ **Udawanie znanych osób lub instytucji** (podawanie się za Bank lub celebrytę).
- ▶ **Błędy w tekście:** literówki, dziwne zdania.

JAK SIĘ BRONIĆ?

- ▶ **Sprawdź nadawcę** – sprawdź kto naprawdę wysłał wiadomość, oszuści często podszywają się pod bank, sklep, celebrytę lub znajomego.
- ▶ **Nie klikaj podejrzanych linków** – link może prowadzić do fałszywej strony, która próbuje ukraść twoje dane lub zainstalować wirusa.
- ▶ **Nie podawaj haseł** – prawdziwe firmy i instytucje nigdy nie proszą o hasło.
- ▶ **Uważaj na ‘pilne’ prośby** – oszuści celowo straszą lub poganiają, żebyś działał szybko i bez zastanowienia.
- ▶ **Zapytaj dorosłego** – jeśli coś wygląda dziwnie lub budzi wątpliwości, lepiej zapytać rodzica lub opiekuna, zanim zareagujesz.

CIEKAWOSTKI

- ▶ Phishing to najczęstszy sposób kradzieży pieniędzy w internecie.
- ▶ Co sekundę wysyłanych jest ponad 100 maili phishingowych.



UŻYWAJ SILNYCH HASEŁ!



NIE DZIEL SIĘ HASŁEM!



STOP! NIE KLIKAJ OD RAZU!



POMYŚL! CZY TA WIADOMOŚĆ LUB SKŁEP WYGLĄDA PODEJRZANIE?



ZAPYTAJ DOROSŁEGO! POKAŻ RODZICOM LUB OPIEKUNOWI



SGH



Uniwersytet
Ekonomiczny
w Katowicach



UNIWERSYTET
EKONOMICZNY
W POZNANIU



UNIWERSYTET
EKONOMICZNY
we Wrocławiu



POLITECHNIKA
GDANSKA



NARODOWY
BANK POLSKI



NARODOWY
BANK POLSKI

Projekt realizowany
z Narodowym Bankiem Polskim
w ramach programu edukacji ekonomicznej