Niebezpieczne transakcje płatnicze, BLIK, oszustwa internetowe i inne zagrożenia w sieci

Referat dla Rodziców wychowanków Zespołu Placówek w Gołotczyźnie

Wprowadzenie

W dzisiejszym świecie cyfrowym, gdzie większość transakcji finansowych odbywa się online, bezpieczeństwo w sieci stało się jednym z kluczowych wyzwań. Wygoda korzystania z aplikacji bankowych, płatności BLIK czy platform zakupowych przyciąga nie tylko użytkowników, ale niestety także cyberprzestępców. W niniejszym referacie omówimy mechanizmy najczęstszych oszustw internetowych związanych z płatnościami, w tym oszustwa BLIK, phishing, malware oraz sposoby ochrony przed tymi zagrożeniami.

Mechanizmy oszustw internetowych

1. Oszustwa BLIK

BLIK, popularny w Polsce system płatności mobilnych, jest jednym z najczęściej wykorzystywanych narzędzi przez oszustów. Mechanizm oszustwa BLIK często opiera się na tzw. *spoofingu* lub *social engineering*, czyli manipulacji ofiarą.

Jak to działa?

- Oszust przejmuje konto ofiary na portalu społecznościowym (np. Facebook).
- Podszywając się pod znajomego, wysyła wiadomość z prośbą o szybki przelew BLIK, np. pod pretekstem nagłego problemu (np. "Zgubiłem portfel, pożycz mi 100 zł").
- Ofiara, ufając znajomemu, podaje kod BLIK, który oszust natychmiast realizuje w bankomacie.

Dlaczego to działa?

- Ofiary często działają w pośpiechu i nie weryfikują tożsamości osoby proszącej o pomoc.
- Brak dodatkowej autoryzacji (np. rozmowy telefonicznej) ułatwia oszustowi realizację transakcji.

2. Phishing

Phishing to jedna z najstarszych i najpowszechniejszych metod wyłudzania danych. Polega na podszywaniu się pod zaufane instytucje (np. banki, firmy kurierskie, platformy zakupowe) w celu wyłudzenia danych logowania, numerów kart kredytowych czy innych poufnych informacji.

Jak to działa?

- Ofiara otrzymuje e-mail lub SMS z linkiem do fałszywej strony internetowej, która wygląda jak strona banku lub firmy.
- Użytkownik, wprowadzając dane logowania, nieświadomie przekazuje je oszustowi.

Cechy charakterystyczne phishingu:

- Pilne wezwania do działania, np. „Twoje konto zostanie zablokowane, jeśli nie zaktualizujesz danych”.
- Błędy językowe lub stylistyczne w treści wiadomości.

- Linki prowadzące do stron o nietypowych adresach URL (np. zamiast www.bank.pl – www.bank123.pl).

3. Malware (złośliwe oprogramowanie)

Złośliwe oprogramowanie to kolejny sposób na przejęcie kontroli nad urządzeniem ofiary. Cyberprzestępcy instalują malware na komputerze lub smartfonie użytkownika, często bez jego wiedzy.

Jak to działa?

- Ofiara pobiera plik zainfekowany złośliwym oprogramowaniem (np. załącznik w e-mailu lub plik z nieznanego źródła).
- Malware może:
    - Przechwytywać dane logowania do bankowości online.
    - Modyfikować dane transakcji (np. zmieniając numer konta odbiorcy).
    - Przejąć pełną kontrolę nad urządzeniem.

4. Fałszywe sklepy internetowe

Cyberprzestępcy tworzą strony internetowe udające legalne sklepy online, oferujące atrakcyjne produkty w niskich cenach. Po dokonaniu płatności ofiara nie otrzymuje zamówienia, a jej dane mogą zostać wykorzystane do dalszych oszustw.

Jak to działa?

- Sklep przyciąga klientów wyjątkowo niskimi cenami.
- Po dokonaniu płatności karta kredytowa ofiary może być obciążana kolejnymi transakcjami, bez jej zgody.

Zagrożenia wynikające z braku świadomości

Wiele z powyższych oszustw odnosi sukces z powodu braku świadomości użytkowników. Ludzie często nie zwracają uwagi na podstawowe zasady bezpieczeństwa, takie jak:

- Nieklikanie w podejrzane linki.
- Weryfikacja tożsamości osób proszących o przelew.
- Korzystanie z aktualnego oprogramowania antywirusowego.

Jak się chronić przed zagrożeniami?

1. **Zasada ograniczonego zaufania**
    - Nigdy nie podawaj kodów BLIK osobom, których tożsamości nie jesteś pewien.
    - Weryfikuj każdą wiadomość z prośbą o pieniądze – najlepiej telefonicznie.
2. **Silne hasła i uwierzytelnianie dwuskładnikowe**
    - Korzystaj z unikalnych, trudnych do odgadnięcia haseł.
    - Włącz uwierzytelnianie dwuskładnikowe (2FA) w każdej aplikacji, która to umożliwia.
3. **Aktualizacje i oprogramowanie antywirusowe**
    - Regularnie aktualizuj system operacyjny i aplikacje.
    - Instaluj sprawdzone oprogramowanie antywirusowe i firewall.

4. **Ostrożność w sieci**
    - Nie klikaj w podejrzane linki, nawet jeśli pochodzą od znajomych.
    - Sprawdzaj adresy URL przed wprowadzeniem danych logowania.
5. **Edukacja i świadomość**
    - Czytaj o najnowszych metodach oszustw i ucz się, jak ich unikać.
    - Uczulaj rodzinę i znajomych na zagrożenia w sieci.

Nieświadome wspieranie wymuszeń – uwaga na prośby dzieci i ich kolegów

W ostatnich latach pojawiło się zjawisko, które dotyczy głównie rodziców uczniów – przekazywanie pieniędzy za pomocą BLIK na prośbę rzekomych kolegów lub koleżanek ich dzieci. Mechanizm tego oszustwa często opiera się na presji emocjonalnej i braku świadomości rodziców.

Jak to wygląda?

- Rodzic otrzymuje wiadomość od dziecka lub jego znajomego z prośbą o szybki przelew BLIK, np. na „ważny zakup" lub „spłatę długu".
- W rzeczywistości takie prośby bywają wymuszeniami, gdzie dzieci, często pod presją rówieśników, proszą rodziców o pieniądze, nie ujawniając prawdziwego charakteru sytuacji.

Dlaczego to niebezpieczne?

- Rodzice, chcąc pomóc, często bez zastanowienia przekazują pieniądze, nie wnikając w szczegóły sytuacji.
- Takie działania mogą wspierać niezdrowe relacje rówieśnicze, w których dzieci są zmuszane do przekazywania pieniędzy lub innych dóbr.

Jak się chronić?

1. Rozmowa z dzieckiem – Regularnie rozmawiaj z dzieckiem o tym, jak radzić sobie z presją rówieśników i dlaczego nie należy ulegać takim prośbom.
2. Weryfikacja prośby – Zawsze sprawdzaj, czy prośba jest uzasadniona. Skontaktuj się bezpośrednio z dzieckiem, aby upewnić się, że rzeczywiście potrzebuje pieniędzy.
3. Edukacja finansowa – Naucz dziecko odpowiedzialności finansowej i tego, jak odmawiać, gdy ktoś próbuje je wykorzystać.

Ważne! Rodzice powinni być czujni i nie traktować każdej prośby o przelew jako pilnej i ważnej. Warto pamiętać, że za takimi sytuacjami mogą stać zarówno oszuści, jak i rówieśnicy wykorzystujący naiwność dziecka lub jego rodziców. Właśnie z tego powodu, aby chronić Wasze dzieci w naszej placówce wprowadzono zakaz przelewów środków pieniężnych na numer konta bankowego i przelewów na telefon BLIK, o czym powiadomiono Rodziców pisemną informacją.

Podsumowanie

Współczesne zagrożenia w sieci, takie jak oszustwa BLIK, phishing czy malware, są wynikiem coraz bardziej zaawansowanych technik stosowanych przez cyberprzestępców. Kluczem do ochrony jest świadomość użytkowników oraz stosowanie podstawowych zasad bezpieczeństwa. Pamiętajmy, że w cyfrowym świecie ostrożność i ograniczone zaufanie mogą uchronić nas przed utratą pieniędzy i danych osobowych.

Opr.Jolanta Myślińska