Program "Klikaj z głową - edukacja cyfrowa ZS3"

PODSZYWANIE SIĘ

METODY DZIAŁANIA, CELE I SPOSOBY OCHRONY

Komisja Przedmiotów Informatycznych
S. P-N.

CZYM JEST PODSZYWANIE SIĘ?

Podszywanie się (ang. impersonation, spoofing) to świadome działanie polegające na fałszywym przedstawianiu się jako inna osoba, instytucja lub podmiot w celu wyłudzenia informacji, pieniędzy lub uzyskania nieautoryzowanego dostępu do zasobów. W erze cyfrowej jest to jedno z najczęstszych przestępstw internetowych.

Podszywanie się może przyjmować formę elektroniczną (e-mail, SMS, media społecznościowe) oraz telefoniczną. Sprawcy działają często w zorganizowanych grupach przestępczych i stale udoskonalają swoje metody.

SKALA ZJAWISKA

Statystyka	Dane
Straty finansowe rocznie (globalnie)	Ponad 10 miliardów USD (wg raportów FBI/IC3)
Najpopularniejszy kanał ataku	E-mail phishing (ok. 80% przypadków)
Wzrost oszustw telefonicznych w Polsce	ok. 40% rok do roku (dane CERT Polska)
Najczęstsza grupa docelowa	Osoby powyżej 60 roku życia
Średnia strata na ofiarę	Od kilkuset do kilkudziesięciu tysięcy złotych

RODZAJE PODSZYWANIA SIĘ W INTERNECIE

PHISHING (E-MAIL)

Phishing to technika, w której atakujący wysyła wiadomość e-mail podszywając się pod zaufaną instytucję (bank, urząd, sklep online, serwis społecznościowy). Celem jest skłonienie ofiary do kliknięcia w fałszywy link lub podania poufnych danych.

Charakterystyczne cechy phishingowych wiadomości:

- Pilny, alarmistyczny ton – np. Twoje konto zostanie zablokowane w ciągu 24 godzin
- Adresy e-mail łudząco podobne do prawdziwych, np. kontakt@pkobp-bezpieczenstwo.pl zamiast pkobp.pl
- Linki prowadzące do fałszywych stron – adres w URL różni się drobnymi szczegółami
- Prośby o podanie loginu, hasła, numerów kart płatniczych lub kodów jednorazowych
- Błędy językowe lub dziwne sformułowania (chociaż AI sprawia, że treści są coraz poprawniejsze)
- Załączniki z wirusami lub złośliwym oprogramowaniem

PRZYKŁAD RZECZYWISTEGO ATAKU PHISHINGOWEGO

- Ofiara otrzymuje e-mail od banku informujący o podejrzanej transakcji.
- Link w mailu prowadzi na stronę identyczną wizualnie z prawdziwą witryną banku.
- Ofiara loguje się – jej dane trafiają bezpośrednio do przestępcy.
- Przestępca w ciągu minut loguje się na prawdziwe konto i wypłaca środki.

SPEAR PHISHING – ATAKI UKIERUNKOWANE

W odróżnieniu od masowego phishingu, spear phishing jest celowany w konkretną osobę lub organizację. Atakujący zbiera wcześniej informacje o ofierze (z LinkedIn, Facebooka, firmowej strony internetowej) i personalizuje wiadomość, co czyni ją bardzo wiarygodna.

- Atakujący zna imię, stanowisko, nazwę firmy i przełożonego ofiary
- Wiadomość może pozorować korespondencję od kolegi lub szefa
- Szczególnie groźny w kontekście firm – może prowadzić do oszustw Business Email Compromise (BEC)

SMISHING (SMS PHISHING)

Smishing to phishing realizowany za pomocą wiadomości SMS. Przestępcy wysyłają fałszywe SMS-y podszywając się pod banki, firmy kurierskie, urzędy skarbowe lub operatorów telekomunikacyjnych.

Typowe scenariusze smishingowe:

- Twoja przesyłka czeka – dopłać 1,29 zł, aby ją odebrać (fałszywa firma kurierska)
- Twoje konto bankowe zostało tymczasowo zablokowane. Kliknij tutaj... (fałszywy bank)
- Urząd Skarbowy: masz do odebrania zwrot podatku. Podaj dane konta.
- Twoja subskrypcja wygasła. Odnów za 1 zł, by nie utracić dostępu.

PODSZYWANIE SIĘ W MEDIACH SPOŁECZNOŚCIOWYCH

Przestępcy tworzą fałszywe profile na portalach społecznościowych (Facebook, Instagram, TikTok, LinkedIn), podszywając się pod:

- Znane osoby publiczne – celebrytów, polityków, influencerów
- Znajomych lub rodzinę ofiary (przejęte lub sklonowane konta)
- Firmy, marki i sklepy oferujące fałszywe promocje
- Organizacje charytatywne zbierające fałszywe datki

Celem może być: wyłudzenie pieniędzy, danych osobowych, intymnych zdjęć (sextortion) lub nakłonienie do inwestycji w fałszywe projekty (np. kryptowaluty).

DEEPFAKE
I PODSZYWANIE SIĘ Z UŻYCIEM AI

Nowoczesne narzędzia sztucznej inteligencji umożliwiają tworzenie realistycznych nagrań wideo i audio z wizerunkiem dowolnej osoby. Deepfake’i są coraz częściej wykorzystywane do:

- Tworzenia fałszywych nagrań wideo od znanych osób zachęcających do inwestycji
- Klonowania głosu – przestępcy mogą zadzwonić, podszywając się głosowo pod szefa lub bliskich
- Fałszywych dowodów na potrzeby szantażu lub manipulacji opinią publiczną

DEEPFAKE
I PODSZYWANIE SIĘ Z UŻYCIEM AI

UWAGA NA KLONOWANIE GŁOSU

- Wystarczy nagranie głosu z 3–10 sekund (z mediów społecznościowych) by AI sklonowała czyjegoś głos.
- Rodziny dostawały już telefony od porwanych dzieci – to nagrania AI, nie prawdziwe rozmowy.
- Firmy doświadczyły przelewy milionowych sum po rozmowie z CEO – który był modelem AI.

PODSZYWANIE SIĘ PRZEZ TELEFON

VISHING – PHISHING GŁOSOWY

Vishing (voice phishing) to technika polegająca na telefonicznym podszywaniu się pod instytucje lub osoby w celu wyłudzenia informacji. Atakujący dzwonią lub nagrywają automatyczne komunikaty (robocalls).

VISHING – PHISHING GŁOSOWY

Najczęstsze scenariusze vishingu:

Scenariusz	Sposób działania
Podszywanie pod bank	Rozmówca twierdzi, że wykryto podejrzaną transakcję i potrzebuje potwierdzenia danych karty lub kodu BLIK
Policjant lub prokurator	Pana/Pani bliski miał wypadek lub jest podejrzany o przestępstwo – potrzebujemy gotówki
Pracownik IT	Pana/Pani komputer jest zainfekowany – proszę zainstalować program zdalnego dostępu
Urząd Skarbowy / ZUS	Ma Pan/Pani zaległości podatkowe – przelej natychmiast lub grozi kara
Metoda na dziecko/wnuczka	Starszy rozmówca udaje dziecko/wnuczka w kryzysie i prosi o gotówkę przez kuriera
Fałszywa infolinia banku	Ofiara jest przekierowywana do przestępcy po wpisaniu numeru w wyszukiwarkę

SPOOFING NUMERÓW TELEFONICZNYCH

Spoofing numeru polega na technicznym podmienieniu numeru wyświetlanego na ekranie odbiorcy.

Dzięki temu:

- Na ekranie telefonu wyświetla się numer prawdziwego banku, policji lub urzędu
- Ofiara widzi numer, który rozpoznaje jako zaufany i nie podejrzewa oszustwa
- Technologia VoIP sprawia, że spoofing jest dostępny i tani dla przestępców

SPOOFING NUMERÓW TELEFONICZNYCH

KLUCZOWA ZASADA

- Żaden bank, policja ani urząd NIE prosi przez telefon o podanie kodów PIN, haseł ani kodów BLIK.
- Wyświetlany numer telefonu NIE gwarantuje tożsamości dzwoniącego – może być sfałszowany.
- Jeśli masz wątpliwości – rozłącz się i sam zadzwoń na oficjalny numer instytucji.

AUTOMATYCZNE POŁĄCZENIA (ROBOCALLS)

Robocalls to automatyczne połączenia telefoniczne z nagranym komunikatem. Stosowane są masowo, gdyż koszt wykonania milionów połączeń jest marginalny. Treści mogą obejmować:

- Informacje o wygranej nagrodzie lub loterii
- Alerty o rzekomych problemach z kontem bankowym lub ubezpieczeniem
- Oferty podejrzanych usług lub produktów
- Groźby prawne (fałszywe wezwania do sądu lub aresztu)

CELE I MOTYWACJE SPRAWCÓW

CELE FINANSOWE

Zdecydowana większość ataków podszycia ma cel finansowy.

Sprawcy dążą do:

- Bezpośredniego wyłudzenia pieniędzy (przelew, BLIK, kryptowaluty, karta podarunkowa)
- Kradzieży danych logowania do kont bankowych
- Uzyskania danych kart płatniczych do nieautoryzowanych transakcji
- Nakłonienia do fałszywych inwestycji (np. platformy crypto, fałszywe fundusze)

KRADZIEŻ TOŻSAMOŚCI

Przestępcy zbierają dane osobowe (PESEL, seria i numer dowodu, adres zamieszkania) by:

- Zaciągać kredyty lub pożyczki na dane ofiary
- Otwierać konta bankowe do prania pieniędzy
- Rejestrować fałszywe firmy lub zawierać umowy
- Sprzedawać tożsamości na czarnym rynku (dark web)

SZPIEGOSTWO I SABOTAŻ KORPORACYJNY

W środowisku biznesowym podszywanie się (szczególnie spear phishing i BEC) służy do:

- Kradzieży poufnych dokumentów, projektów i patentów
- Uzyskania dostępu do systemów informatycznych firmy
- Zakłócenia działalności konkurencji lub instytucji
- Szantażu i wymuszenia okupu za odszyfrowanie danych (ransomware)

SEXTORTION I SZANTAŻ

Podszywanie się pod atrakcyjne osoby w mediach społecznościowych lub aplikacjach randkowych bywa wstępem do:

- Nakłonienia do przesłania intymnych zdjęć lub filmów
- Szantażu – groźba upublicznienia materiałów, jeśli ofiara nie zapłaci
- Długotrwałej manipulacji emocjonalnej (romance scam)

DEZINFORMACJA I WPŁYWANIE NA OPINIĘ PUBLICZNĄ

Podszywanie się jest też narzędziem politycznym i propagandowym:

- Tworzenie fałszywych profili osób publicznych do szerzenia dezinformacji
- Podszywanie się pod dziennikarzy lub media w celu rozpowszechniania fałszywych informacji
- Operacje wpływu – skoordynowane nieautentyczne zachowania na platformach społecznościowych

JAK ROZPOZNAĆ PRÓBĘ PODSZYWANIA SIĘ?

SYGNAŁY OSTRZEGAWCZE – CZERWONE FLAGI

CZERWONE FLAGI – natychmiast reaguj!

- Presja czasu: Musisz działać TERAZ, inaczej stracisz pieniądze/konto/wolność
- Prośba o podanie kodu BLIK, PIN, hasła lub kodu jednorazowego
- Żądanie przelewu na bezpieczne konto lub zakupu kart podarunkowych
- Rozmówca prosi o zainstalowanie aplikacji zdalnego dostępu (AnyDesk, TeamViewer)
- Link w e-mailu lub SMS prowadzi na dziwną, nieznaną stronę internetową
- Wiadomość pochodzi od znajomego, który nagle prosi o pieniądze lub dane
- Oferta jest zbyt atrakcyjna, żeby była prawdziwa
- Rozmówca zna Twoje dane (imię, adres) – to nie dowód, że jest prawdziwy!

JAK WERYFIKOWAĆ TOŻSAMOŚĆ ROZMÓWCY?

- Rozłącz się i oddzwoń na oficjalny numer – znajdź go samodzielnie na stronie instytucji
- Nigdy nie klikaj w linki z SMS-ów ani e-maili – wpisz adres strony ręcznie w przeglądarce
- Sprawdź adres URL strony – fałszywe strony mają subtelnie zmienione adresy
- Skontaktuj się bezpośrednio ze znajomym innym kanałem (np. zadzwoń, jeśli dostałeś podejrzanego SMS-a)
- Pamiętaj: wyświetlany numer telefonu może być sfałszowany

WERYFIKACJA WIADOMOŚCI E-MAIL

Co sprawdzić	Jak to zrobić
Adres nadawcy	Sprawdź PEŁNY adres e-mail, nie tylko wyświetlaną nazwę
Linki w treści	Najedź kursorem na link – sprawdź adres w lewym dolnym rogu przeglądarki
Certyfikat SSL strony	Szukaj kłódki i https:// – ale pamiętaj, że fałszywe strony też mogą go mieć
Nagłówki e-maila	Zaawansowani użytkownicy mogą sprawdzić pola SPF, DKIM, DMARC
Zawartość wiadomości	Bądź podejrzliwy wobec pilnych próśb i błędów językowych

JAK SIĘ CHRONIĆ?

ZASADY HIGIENY CYFROWEJ

DOBRE PRAKTYKI – stosuj na co dzień

- Używaj silnych, unikalnych haseł dla każdego serwisu (menedżer haseł: Bitwarden, 1Password)
- Włącz uwierzytelnianie dwuskładnikowe (2FA) wszędzie gdzie to możliwe
- Regularnie aktualizuj system operacyjny, przeglądarkę i aplikacje
- Korzystaj z renomowanego oprogramowania antywirusowego
- Nie podłączaj nieznanych urządzeń USB do komputera
- Regularnie twórz kopie zapasowe ważnych danych
- Bądź ostrożny przy korzystaniu z publicznych sieci Wi-Fi (używaj VPN)
- Ogranicz dane osobowe udostępniane publicznie w mediach społecznościowych

OCHRONA
PRZED PHISHINGIEM E-MAIL

- Nie klikaj w linki w podejrzanych wiadomościach
- Nie otwieraj załączników od nieznanych nadawców
- Używaj filtrów antyspamowych i antyphishingowych
- Zgłaszaj podejrzane wiadomości do dostawcy poczty (przycisk Zgłoś phishing)
- Banki i urzędy NIGDY nie proszą o podanie haseł przez e-mail

OCHRONA
PRZED VISHINGIEM I SMISHINGIEM

- Nie odpowiadaj na nieznane numery i nie oddzwaniaj na podejrzane numery
- Zainstaluj aplikację do blokowania podejrzanych połączeń (np. Truecaller)
- Sprawdź numer w wyszukiwarce – ofiary oszustów często opisują swoje doświadczenia online
- Ustal z rodziną hasło awaryjne do weryfikacji tożsamości w sytuacjach kryzysowych

OCHRONA DANYCH OSOBOWYCH

- Udostępniaj numer PESEL i dane dowodu tylko gdy jest to absolutnie konieczne
- Monitoruj swój raport BIK – sprawdźaj, czy ktoś nie zaciąga kredytów na Twoje dane
- Zastrzeż swój PESEL w systemie Ministerstwa Finansów (www.gov.pl/zastrzezenie-peselu)
- Chroń zdjęcia dokumentów tożsamości – nie wysyłaj ich przez komunikatory

CO ZROBIĆ, GDY PADNIESZ OFIARĄ?

KROKI NATYCHMIASTOWE

1. ZATRZYMAJ działanie – nie podejmuj dalszych kroków sugerowanych przez oszusta
2. Skontaktuj się z bankiem – zadzwoń na infolinię i zablokuj kartę/konto. Działaj w ciągu minut!
3. Zmień hasła – do konta e-mail, bankowości online i wszystkich ważnych serwisów
4. Zbierz dowody – zachowaj wiadomości, zrzuty ekranu, numery telefonów
5. Zgłoś na policję – złóż zawiadomienie o przestępstwie (art. 190a KK, art. 286 KK)
6. Zgłoś do CERT Polska – cert.pl lub tel. 799 448 084

ZGŁASZANIE PHISHINGU

Instytucja	Kontakt / Sposób zgłoszenia
CERT Polska	incydent.cert.pl lub SMS 8080 (fałszywe SMS-y)
Policja	Komenda policji lub e-policja.pl
UOKiK (fałszywe sklepy)	uokik.gov.pl/zawiadomienie
Bank	Infolinia banku – numer na karcie lub stronie oficjalnej
Google (fałszywe strony)	safebrowsing.google.com/safebrowsing/report_phish
Social media (fałszywe profile)	Opcja “Zgłoś” bezpośrednio przy profilu

ASPEKTY PRAWNE

PRZEPISY POLSKIEGO PRAWA

Podszywanie się i powiązane działania są przestępstwami ścigane z mocy prawa:

Przepis	Opis przestępstwa i kara
Art. 190a § 2 Kodeksu Karnego	Podszywanie się pod inną osobę w celu wyrządzenia szkody – do 3 lat pozbawienia wolności
Art. 286 § 1 KK	Oszustwo – do 8 lat pozbawienia wolności (przy dużej wartości szkody)
Art. 267 KK	Nieuprawniony dostęp do danych – do 2 lat pozbawienia wolności
Art. 294 KK	Oszustwo na dużą skalę – do 10 lat pozbawienia wolności
RODO / UODO	Nielegalne przetwarzanie danych osobowych – kary finansowe i/lub karne

ODPOWIEDZIALNOŚĆ BANKÓW

Na mocy dyrektywy PSD2 i przepisów krajowych, banki mają obowiązek stosowania silnego uwierzytelniania (SCA). W przypadku nieautoryzowanych transakcji bank jest co do zasady zobowiązany do zwrotu środków, chyba że udowodni, że klient działał z rażącym niedbalstwem lub celowo.

DZIĘKUJEMY ZA UWAGĘ