INŻYNIERIA SPOŁECZNA

Mechanizmy • phishing • spear phishing

2 × 45 MINUT

TECHNIK CYBERBEZPIECZEŃSTWA

Zrozum atak.
Rozpoznaj sygnały.

Na podstawie literatury naukowej, NIST, CERT Polska i materiału z udostępnionych stron książki.

CELE I CZAS

Plan dwóch lekcji

00–10	Wprowadzenie i definicje
10–25	Psychologia manipulacji
25–45	Phishing i analiza adresów
45–62	Spear phishing i scenariusze
62–78	Weryfikacja i reakcja
78–90	Quiz i omówienie

ROZMOWA / 3 MIN

Na rozgrzewkę: klikniesz czy sprawdzisz?

SMS: „Twoja paczka nie może zostać doręczona.”

Dopłać 1,49 zł w ciągu 30 minut, inaczej wróci do nadawcy.

Pytanie: co w tej treści ma wpłynąć na Twoją decyzję?

DEFINICJA

Inżynieria społeczna = manipulacja człowiekiem

Atakujący nie musi łamać hasła. Może skłonić człowieka, aby je ujawnił.

CEL

Dane, pieniądze, dostęp lub wykonanie działania.

NARZĘDZIE

Zaufanie, emocje, kontekst i wiarygodna historia.

EFEKT

Odbiorca sam realizuje zamiar oszusta.

NIST CSRC, hasło „social engineering”.

SCHEMAT

Model działania ataku socjotechnicznego

01

PRETEKST

„Piszę z sekretariatu”

→

02

BODZIEC

„Konto zostanie wyłączone”

→

03

ŻĄDANIE

„Potwierdź dostęp”

→

04

DZIAŁANIE

Kliknięcie / podanie danych

→

05

SKUTEK

Przejęcie konta / strata

Najważniejszy element: wymuszenie konkretnej decyzji.

Opracowanie dydaktyczne na podstawie NIST i Spicer & Nurse (2026).

To nie „głupota” — to przetwarzanie informacji

Szybka ocena

„Znam logo, znajomy pisze, treść brzmi normalnie”.

Mózg korzysta z prostych wskazówek, bo oszczędza uwagę.

Świadoma weryfikacja

„Czy prośba jest oczekiwana? Czy dane zgadzają się z niezależnym źródłem?”.

Zatrzymanie decyzji daje czas na sprawdzenie.

Vishwanath i in. (2011); Spicer & Nurse (2026).

Mechanizmy wpływu — część 1

AUTORYTET

„Dyrektor IT poleca…”

Fałszywy przełożony lub specjalista ma zmniejszyć opór.

NIEDOSTĘPNOŚĆ

„Tylko do 16:00!”

Ograniczony czas lub liczba miejsc utrudniają namysł.

SYMPATIA

„Jestem kolegą Twojego kolegi”.

Wspólne zainteresowania mogą wzmacniać zaufanie.

Griskevicius & Cialdini (2010), DOI: 10.1002/9781444316568.wiem03047.

Mechanizmy wpływu — część 2

WZAJEMNOŚĆ

„Dałem Ci prezent — teraz podaj dane do wysyłki”.

Poczucie zobowiązania.

DOWÓD SPOŁECZNY

„Wszyscy z klasy już potwierdzili konta”.

Naśladowanie innych.

KONSEKWENCJA

„Zacząłeś rejestrację, dokończ ją”.

Chęć domknięcia decyzji.

Griskevicius & Cialdini (2010).

Badania: reakcja na phishing jest zależna od kontekstu

54 BADANIA

W przeglądzie z 2026 r. wybrano 54 badania spośród 4402 wyszukanych publikacji.

Wniosek: nie istnieje jedna prosta cecha „łatwej ofiary”.

NIE MA JEDNEJ REGUŁY

Autorytet, treść i okoliczności wpływają na ocenę wiarygodności.

Silna presja bywa też sygnałem ostrzegawczym.

Wiedza zwiększa szanse obrony, ale sama nie zastępuje bezpiecznych procedur.

Spicer & Nurse (2026); Baryshevtsev & McGlynn (2020); Auton & Sturman (2025).

Phishing: fałszywa prośba od zaufanego nadawcy

Phishing = podszywanie się + zwodnicza prośba + ryzyko straty.

PODSZYWA SIĘ

Bank, kurier, sklep, urząd, szkoła, znajomy.

KUSI / STRASZY

Dopłata, blokada, prezent, nagroda, pilny problem.

WYMUSZA

Logowanie, płatność, kod, instalację, udostępnienie pliku.

NIST CSRC: phishing; CERT Polska — Rozpoznanie phishingu.

Nie tylko e-mail: te same mechanizmy, różne kanały

@

E-MAIL

Fałszywy faktura / aktualizacja

...

SMS / MESSENGER

Dopłata lub wiadomość od znajomego



TELEFON

Rzekomy pracownik banku

QR

QR / REKLAMA

Przekierowanie na cudzą stronę

Anatomia wiadomości phishingowej

OD: Sekretariat <powiadomienie@weryfikacja-konta.test>

TEMAT: Pilne potwierdzenie konta ucznia

W związku z aktualizacją dziennika konto zostanie zablokowane za 60 minut. Zaloguj się poprzez załączony odnośnik, aby zachować dostęp.

POTWIERDŹ KONTO

Fikcyjna wiadomość — nie jest prawdziwym adresem ani przyciskiem.

Scenariusz fikcyjny; typowe cechy opisuje CERT Polska.

UMIEJĘTNOŚĆ PRAKTYCZNA

Co jest domeną, a co tylko jej fragmentem?

https://konto.szkola.example/logowanie

https://szkola.example.weryfikacja.test/logowanie

Pierwszy adres → szkola.example • Drugi adres → weryfikacja.test

Adresy są fikcyjne i służą wyłącznie do analizy.

CERT Polska — Rozpoznanie phishingu; materiał książkowy, s. 71–74.

HTTPS i kłódka ≠ potwierdzenie uczciwości strony

HTTPS chroni połączenie

Szyfruje dane w drodze do serwera i pozwala sprawdzić, z jaką domeną nawiązano chronioną sesję.

HTTPS nie rozstrzyga

Czy odbiorca po drugiej stronie jest prawdziwym bankiem, sklepem, szkołą lub urzędem.

CERT Polska; NIST SP 800-63B-4.

Checkpoint: trzy pytania przed logowaniem

01 Czy prośba była oczekiwana?

02 Czy znam prawidłową domenę usługi?

03 Czy mogę sprawdzić informację inną drogą?

CERT Polska, rozpoznawanie phishingu.

Spear phishing — atak dopasowany do odbiorcy

Phishing masowy

„Drogi Kliencie, Twoja paczka jest zatrzymana. Dopłać 1,49 zł”.

Spear phishing

„Pani Anno, faktura za drukarki zamówione dla pracowni TI wymaga zatwierdzenia”.

ENISA, Phishing/Spear phishing; NIST Small Business Glossary.

Skąd bierze się wiarygodność spear phishingu?

PUBLICZNE INFORMACJE

Plan wydarzeń, ogłoszenia, nazwy działów, wpisy w mediach społecznościowych.

PRAWDOPODOBNA HISTORIA

Prośba pasuje do codziennych obowiązków konkretnej osoby.

FAŁSZYWY NADAWCA

Podszycie się pod współpracownika, dostawcę lub sekretariat.

ENISA; materiał książkowy R. Kruczek, s. 75–78.

PRZYKŁAD SZKOLNY

Studium przypadku: „faktura za drukarki”

Od: Dostawca sprzętu <rozliczenia@faktury-szkolne.test>

Temat: Zamówienie 2 drukarek 3D — pilna korekta

Dzień dobry,

zgodnie z rozmową dotyczącą pracowni proszę potwierdzić nowe konto do płatności. Termin przelewu mija dziś o 15:00.

Dział rozliczeń

Co dokładnie trzeba zweryfikować przed jakimkolwiek przelewem?

Fikcyjna sytuacja dydaktyczna na podstawie typologii ENISA.

Spear phishing ≠ „bezbłędny e-mail”

- Poprawna polszczyzna nie dowodzi autentyczności.
- Znajomość Twojego imienia nie oznacza, że nadawca Cię zna.
- Wiadomość z prawdziwego konta znajomego może być oszustwem.
- Prośba o przelew lub logowanie wymaga niezależnego potwierdzenia.

Spicer & Nurse (2026); CERT Polska — Rozpoznanie phishingu.

Techniki podszywania się: czego szukać?

PODOBNA DOMENA

literówka, dodatkowy człon

NADAWCA / REPLY-TO

nazwa nadawcy to nie dowód

ZAŁĄCZNIK

plik lub makro z poleceniem uruchomienia

KOD QR

ukryty do chwili skanowania adres

Materiał książkowy, s. 71–79; CERT Polska.

Najbezpieczniejszy nawyk: przerwij → zweryfikuj

1	**ZATRZYMAJ SIĘ**	Nie reaguj automatycznie na presję.
2	**SPRAWDŹ ADRES**	Oceń faktyczną domenę, nie samą nazwę.
3	**ZWERYFIKUJ**	Wejdź ręcznie / z zakładki / zadzwoń na znany numer.
4	**NIE POTWIERDZAJ**	Nie podawaj kodów i nie zatwierdzaj nieznanych operacji.

CERT Polska; ENISA; NIST 800-63B-4.

Co zrobić, jeśli ktoś już podał dane?

- Hasło → zmień na prawdziwej stronie, zakończ sesje, włącz MFA.
- Dane karty / kod płatności → natychmiast skontaktuj się z bankiem.
- Przejęte konto → ostrzeż kontakty i zgłoś administratorowi.
- Podejrzany plik → nie uruchamiaj dalej; zgłoś incydent.

ZGŁOŚ: INCYDENT.CERT.PL

SMS → 8080

Dlaczego sama czujność nie wystarczy?

CZŁOWIEK

Zatrzymuje reakcję, sprawdza adres i treść żądania.

PROCEDURA

Zmianę konta do przelewu potwierdzamy niezależnym kanałem.

TECHNOLOGIA

Passkeys/FIDO2, zabezpieczenia poczty i kont, aktualizacje.

Spicer & Nurse (2026); NIST SP 800-63B-4.

Ćwiczenie: która prośba wymaga dodatkowej kontroli?

A • SMS

„Odebranie przesyłki: dopłata 1,49 zł. Otwórz link w ciągu 10 minut”.

B • E-MAIL

„Dzień dobry, w związku z korektą faktury proszę potwierdzić nowy rachunek bankowy”.

Pytanie: czym różnią się mechanizmy perswazji? Jak sprawdzisz A i B?

Dwie przykładowe wiadomości fikcyjne.

5 zasad do zapamiętania

1. Atak manipuluje decyzją — nie tylko komputerem.
2. Phishing bywa masowy; spear phishing jest celowany.
3. Wiarygodne szczegóły i HTTPS nie dowodzą autentyczności.
4. Dane i płatności sprawdzaj przez niezależny kanał.
5. Zgłaszaj incydenty: CERT Polska, szkolny administrator.

NIST; CERT Polska; przegląd Spicer & Nurse (2026).

Quiz końcowy: czy rozpoznasz manipulację?

10 pytań • ABCD • 1 prawidłowa odpowiedź

Odpowiedz samodzielnie. Uzasadnij swój wybór.

Pytania autorskie oparte na przedstawionych definicjach i przykładach.

Quiz — pytanie 1 z 10

PYTANIE 1

Czym jest inżynieria społeczna?

A. Łamaniem szyfru Wi-Fi metodą brute force

B. Manipulowaniem ludźmi w celu uzyskania działania lub informacji

C. Testowaniem zapory sieciowej

D. Wyłącznie instalowaniem wirusów

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 2 z 10

PYTANIE 2

„Dyrektor poleca natychmiast zmienić hasło”. Jaki mechanizm jest najbardziej widoczny?

A. Wzajemność

B. Dowód społeczny

C. Autorytet

D. Sympatia

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 3 z 10

PYTANIE 3

Co najlepiej odróżnia spear phishing od masowego phishingu?

A. Spear phishing działa tylko przez SMS

B. Spear phishing jest dopasowany do konkretnej osoby lub instytucji

C. Spear phishing zawsze zawiera wirusa

D. Spear phishing nie używa e-maila

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 4 z 10

PYTANIE 4

Który adres ma domenę szkola.example?

A. https://konto.szkola.example

B. https://szkola.example.konto.test

C. https://szkola-example.test

D. https://konto-szkola.test

Quiz — pytanie 5 z 10

PYTANIE 5

O czym świadczy kłódka HTTPS przy pasku adresu?

A. Że witryna została zatwierdzona przez bank

B. Że właściciel strony nie jest oszustem

C. Że każde polecenie na stronie jest bezpieczne

D. Że połączenie z daną domeną jest zabezpieczone

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 6 z 10

PYTANIE 6

Ktoś prosi e-mailem o pilną zmianę rachunku do przelewu. Co robić?

A. Wykonać przelew, skoro zna kwotę faktury

B. Potwierdzić zmianę przez wcześniej znany, niezależny kanał

C. Poprosić o drugiego e-maila z tego samego adresu

D. Odpowiedzieć na e-mail i zapytać o zgodę

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 7 z 10

PYTANIE 7

Która cecha najlepiej opisuje wiarygodną wiadomość spear phishingową?

A. Musi zawierać błędy ortograficzne

B. Zawsze pochodzi z nowego, nieznanego konta

C. Może wykorzystywać prawdziwe dane o odbiorcy

D. Nie może naśladować znajomego

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 8 z 10

PYTANIE 8

Co może być celem phishingu oprócz kradzieży hasła?

A. Wyłudzenie kodu płatności lub wykonanie przelewu

B. Wyłącznie zwiększenie liczby reklam

C. Wyłącznie spowolnienie sieci

D. Tylko instalacja aktualizacji systemu

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 9 z 10

PYTANIE 9

Podałeś hasło na fałszywej stronie. Jaka reakcja jest właściwa?

A. Czekać, aż konto samo się zablokuje

B. Odpisać autorowi wiadomości z prośbą o skasowanie danych

C. Zmienić hasło na prawdziwej stronie, wylogować sesje i zgłosić incydent

D. Wysłać takie samo hasło administratorowi SMS-em

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Quiz — pytanie 10 z 10

PYTANIE 10

Gdzie w Polsce można przekazać podejrzany SMS?

A. Na numer 112

B. Na numer 8080

C. Na numer 997

D. Na numer 8000

Pytania autorskie: definicje NIST, CERT Polska, ENISA.

Klucz odpowiedzi i krótkie wyjaśnienie

01 B • Manipulacja decyzją

02 C • Autorytet

03 B • Atak celowany

04 A • Właściwa domena

05 D • Szyfrowane połączenie

06 B • Niezależna weryfikacja

07 C • Prawdziwe dane odbiorcy

08 A • Kod / przelew

09 C • Zmiana hasła i zgłoszenie

10 B • Numer 8080

Źródła do uzasadnienia: NIST, ENISA, CERT Polska, badania przywołane wcześniej.

Literatura naukowa (1/2)

Spicer, M., Nurse, J. R. C. (2026). What makes people susceptible to phishing attacks: A systematic literature review. Computers & Security. DOI: 10.1016/j.cose.2026.105096

Vishwanath, A. i in. (2011). Why do people get phished? Decision Support Systems, 51(3), 576–586. DOI: 10.1016/j.dss.2011.03.002

Griskevicius, V., Cialdini, R. B. (2010). Social Influence. Wiley International Encyclopedia of Marketing. DOI: 10.1002/9781444316568.wiem03047

Baryshevtsev, M., McGlynn, J. (2020). Persuasive Appeals Predict Credibility Judgments of Phishing Messages. Cyberpsychology, Behavior, and Social Networking, 23(5), 297–302. DOI: 10.1089/cyber.2019.0592

Źródła zweryfikowane online 15.11.2026.

Literatura i instytucje (2/2)

Auton, J. C., Sturman, D. (2025). Persuasion under pressure. Information and Computer Security, 33(5), 845–859. DOI: 10.1108/ICS-07-2024-0163

Jansson, K., von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593. DOI: 10.1080/0144929X.2011.632650

NIST CSRC: csrc.nist.gov/glossary/term/phishing • NIST SP 800-63B-4: pages.nist.gov/800-63-4/sp800-63b.html

CERT Polska: wiedza.cert.pl/bezpieczenstwo-osobiste/rozpoznanie-phishingu/ • incydent.cert.pl • SMS 8080

Materiał uzupełniający: Robert (ProXy) Kruczek, „Phishing: techniki ataku”, udostępnione fotografie s. 67–85 i 92.

Jeden najważniejszy nawyk

**Gdy wiadomość naciska na natychmiastowe działanie,
sprawdź ją poza kanałem, którym przyszła.**

ZAUFAJ PROCEDURZE WERYFIKACJI — NIE SAMEMU KOMUNIKATOWI.