

## Wiadomości E-mail:

Cecha	Phishing	Non-phishing
Nadawca (adres e-mail)	ulubione@allegro.com (podejrzany – litery podmienione)	ulubione@allegro.pl (zaufany – oficjalny adres firmy)
Domena	allegro.com (podejrzana – podobna do prawdziwej, ale z podmianami znaków)	allegro.pl (zaufana – oficjalna domena firmy)
Szyfrowanie TLS	Brak szyfrowania TLS (brak kłódki, niezabezpieczone połączenie)	Szyfrowanie TLS (bezpieczne połączenie, widoczna kłódka)
Załącznik	Nieoczekiwany załącznik (np. .exe, .zip, makra)	Brak załącznika lub oczekiwany (np. faktura PDF)
Błędy językowe	Obecne błędy językowe (ortograficzne, gramatyczne)	Brak błędów językowych (poprawny język)
Presja psychologiczna	Wzbudzanie strachu lub pilności („Twoje konto zostanie zablokowane”)	Brak presji, spokojny ton wiadomości
Podejrzany link	Link do fałszywej strony (np. zmieniona domena, literówki)	Link do prawdziwej, znanej strony (np. <a href="https://allegro.pl/">https://allegro.pl/...</a> )
Personalizacja	Brak personalizacji („Drogi użytkowniku”)	Spersonalizowana treść (np. imię, nazwisko, numer zamówienia)

## Wiadomości SMS:

Cecha	Phishing (SMS)	Non-phishing (SMS)
Nadawca	Numer lub adres nadawcy wygląda podejrzanie (np. losowy ciąg cyfr, nieznan nadawca, nieznan numer)	Numer lub nazwa nadawcy jest znana i zaufana (np. „Allegro”, „Bank XYZ”)
Błędy językowe	Błędy ortograficzne lub gramatyczne (nienaturalne sformułowania)	Wiadomość poprawna językowo (gramatyka i ortografia bez zarzutu)
Presja psychologiczna	Wywoływanie strachu lub pilności (np. „Pilne!”, „Zablokujemy konto!”)	Spokojna treść bez straszenia (np. informacyjna wiadomość od instytucji)
Linki	Link prowadzi do podejrzanej lub nieznannej strony (dziwna domena)	Link prowadzi do oficjalnej strony lub brak linku

<b>Personalizacja</b>	Brak personalizacji (np. „Szanowny Kliencie”)	Zawiera dane indywidualne (np. imię, nazwisko, numer klienta)
<b>Inne</b>	Inne: np. zbyt dobra oferta, obietnica nagrody, brak kontaktu zwrotnego	Inne: np. numer kontaktowy do firmy, zgodność z historią komunikacji

## Strony WWW:

Cecha	Phishing (strona WWW)	Non-phishing (strona WWW)
<b>Szyfrowanie SSL (HTTP)</b>	Brak szyfrowania SSL – adres zaczyna się od http://, brak kłódki lub kłódka przekreślona / czerwona	Szyfrowanie SSL – adres zaczyna się od https://, kłódka zielona lub normalna
<b>Domena</b>	Podejrzana domena – literówki, dodatkowe znaki, dziwne rozszerzenia (np. .xyz, .top, a1legro.xyz.org)	Zaufana domena – oficjalna, poprawna domena znanej marki (np. allegro.pl)
<b>Załącznik</b>	Strona wymaga pobrania podejrzanego pliku (np. faktura.exe, dokument.zip)	Brak załącznika lub tylko znane, bezpieczne pliki (np. PDF regulaminu)
<b>Błędy językowe</b>	Widoczne błędy językowe – ortograficzne, gramatyczne, nienaturalne sformułowania	Brak błędów językowych – profesjonalnie przygotowany tekst
<b>Presja psychologiczna</b>	Treści wywołujące strach lub pośpiech (np. „Twoje konto zostanie usunięte!”)	Spokojna, informacyjna treść, brak nacisków
<b>Podejrzany link</b>	Linki przekierowujące na nieznane, dziwne domeny (np. kliknij-tutaj-zabezpiecz.com)	Linki prowadzą do zaufanych i znanych stron

## Reklamy:

Cecha	Phishing (reklama)	Non-phishing (reklama)
<b>Domena</b>	Podejrzana domena (adres zawiera literówki, dziwne znaki lub nie pasuje do marki)	Zaufana domena (adres zgodny z oficjalną stroną znanej firmy)
<b>Błędy językowe</b>	Obecne błędy (ortograficzne, gramatyczne, niezrozumiały tekst)	Brak błędów (tekst poprawny, zgodny z normami językowymi)
<b>Presja psychologiczna</b>	Stosowanie presji (np. „Pilne!”, „Twoje konto zostanie zablokowane”)	Brak presji (normalna treść bez straszenia i pośpiechu)
<b>Podejrzany link</b>	Link prowadzi do nieznanej lub podejrzanej strony	Link prowadzi do oficjalnej, wiarygodnej strony
<b>Inne</b>	Inne: Np. zbyt atrakcyjna oferta („iPhone za 1 zł”), brak danych kontaktowych	Inne: Np. pełne dane firmy, oferta realistyczna, linki do regulaminów i polityk

## Posty w mediach społecznościowych:

Cecha	Phishing (post)	Non-phishing (post)
Nadawca	Nieznany lub podejrzany nadawca (np. dziwna nazwa profilu, brak historii aktywności)	Zaufany nadawca (znana firma, osoba, oficjalny profil z weryfikacją)
Załącznik	Post zawiera plik do pobrania (np. .zip, .exe) – może być niebezpieczny	Brak załącznika – nie zawiera plików do pobrania
Błędy językowe	Widoczne błędy ortograficzne, gramatyczne, dziwne sformułowania	Tekst poprawny językowo, profesjonalnie napisany
Presja psychologiczna	Treść wzbudza pilność, strach lub zagrożenie (np. „Kliknij natychmiast!”)	Post spokojny, informacyjny, nie wywołuje niepokoju
Podejrzany link	Link prowadzi do nieznanej, dziwnej strony	Brak linków lub link prowadzi do znanej, wiarygodnej strony
Formularz	Post prosi o dane wrażliwe lub finansowe (np. poprzez podejrzany formularz, napisanie danych w komentarzu lub poprzez prywatną wiadomość)	Brak formularza – post nie wymaga podawania danych
Inne	Inne: np. zbyt atrakcyjna oferta, brak komentarzy, brak reakcji użytkowników	Inne: np. realistyczna treść, aktywność użytkowników, komentarze, polubienia

