

Test phishingowy: 10 wiadomości do rozpoznania

Do przejścia z zespołem na najbliższym spotkaniu. Zajmuje 20 minut.

Jak to przeprowadzić: rozdaj strony z wiadomościami, **klucz zatrzymaj dla siebie**. Każdy pracuje sam przez 10 minut i przy każdej wiadomości pisze ATAK albo OK. Potem czytasz klucz na głos. Nie chodzi o wynik jednej osoby — chodzi o to, żeby wszyscy usłyszeli, po czym to się poznaje.

Uwaga: nie wszystkie wiadomości są atakiem. Zespół, który zaznaczy „atak” przy wszystkich dziesięciu, jest równie bezużyteczny jak taki, który klika we wszystko — zablokuje zwykłą pracę firmy.

Wiadomość 1

Od: Krajowy System e-Faktur ksef-powiadomienia@ksef.gov.pl **Temat:** Nowa faktura oczekuje na pobranie — KSeF/2026/084121

Szanowni Państwo, w systemie KSeF oczekuje nowy dokument wystawiony przez Państwa kontrahenta. Dokument należy pobrać w ciągu 7 dni. **[POBIERZ FAKTURĘ]**

ATAK / OK:

Wiadomość 2

Od: Anna Wiśniewska (biuro rachunkowe) a.wisniewska@biuro-rach.com.pl **Temat:** Re: Re: dokumenty za sierpień

Dzień dobry, brakuje mi jeszcze wyciągu z rachunku firmowego za sierpień. Może być PDF z bankowości. Zamykam sierpień w piątek. Pozdrawiam, Anna

ATAK / OK:

Wiadomość 3

Od: DPD Polska no-reply@dpd-dostawa.info **SMS:** Twoja przesyłka została zatrzymana. Wymagana dopłata 2,30 zł do opłaty celnej: dpd-oplata.info/pl

ATAK / OK:

Wiadomość 4

Od: Marek Kowalczyk (prezes) m.kowalczyk@firma-sp-zoo.com **Temat:** pilne, jestem na spotkaniu

Jesteś przy komputerze? Potrzebuję, żebyś wykonała dzisiaj przelew do nowego dostawcy, kwota 18 400 zł. Jestem na spotkaniu do 16, nie mogę rozmawiać — pisz mailem. Dane rachunku wysyłam za chwilę. Sprawa poufna, nie omawiaj tego z resztą biura.

ATAK / OK:

Wiadomość 5

Od: Tomasz Bąk (dostawca, stały kontrahent) t.bak@stalowmet.pl **Temat:** Faktura FV 448/09/2026 — UWAGA zmiana numeru konta

Dzień dobry, w załączeniu faktura za wrzesień. Informujemy, że od tego miesiąca zmieniliśmy bank — proszę o płatność na nowy rachunek podany na fakturze. Stary rachunek został już zamknięty.

ATAK / OK:

Wiadomość 6

Od: Microsoft 365 security@microsoft-alert365.com **Temat:** Twoje hasło wygasa dzisiaj

Hasło do konta w domenie Twojej firmy wygasa za 4 godziny. Aby zachować dostęp do poczty, potwierdź hasło pod poniższym adresem. W przeciwnym razie konto zostanie zawieszona. **[ZACHOWAJ OBECNE HASŁO]**

ATAK / OK:

Wiadomość 7

Od: mBank kontakt@mbank.pl **Temat:** Potwierdzenie wykonania przelewu

Informujemy o wykonaniu przelewu na kwotę 4 900,00 zł na rachunek PL61 1090 ** 3021. Jeżeli to nie Ty, skontaktuj się z nami przez aplikację lub infolinię podaną na odwrocie karty.

ATAK / OK:

Wiadomość 8

Od: Zespół rozliczeń billing@notion-invoices.net **Temat:** Nieopłacona subskrypcja — utrata historii za 48 godzin

Płatność za Twój plan nie została zrealizowana. Jeżeli nie uregulujesz jej w ciągu 48 godzin, Twoje konto zostanie usunięte razem z całą historią dokumentów i rozmów. **[OPŁAĆ TERAZ]**

ATAK / OK:

Wiadomość 9

Od: Kadry kadry@nasza-firma.pl **Temat:** Regulamin pracy zdalnej — proszę o zapoznanie

Dzień dobry, w załączeniu zaktualizowany regulamin pracy zdalnej obowiązujący od 1 października. Proszę o zapoznanie się i potwierdzenie mailem do końca tygodnia. Załącznik: regulamin-pracy-zdalnej.pdf

ATAK / OK:

Wiadomość 10

Od: Dział windykacji windykacja@e-faktura-24.pl **Temat:** Wezwanie do zapłaty — załącznik: naleznosc_09_2026.zip

W załączeniu przesyłamy wezwanie do zapłaty wraz z fakturą. Prosimy o pilne uregulowanie należności w terminie 3 dni, w przeciwnym razie sprawa zostanie skierowana na drogę sądową.

ATAK / OK:

Klucz odpowiedzi — dla osoby prowadzącej

Czytaj na głos po tym, jak wszyscy skończą. Przy każdej pozycji podana jest **jedna rzecz**, która przesądza sprawę. Jeżeli zespół zapamięta tylko te dziesięć zdań, test spełnił swoje zadanie.

Nr	Odpowiedź	Co przesądza
1	ATAK	Domena ksef-gov.pl nie jest domeną państwową. Dokumenty pobierasz po zalogowaniu na platformę, nigdy z linka w mailu
2	OK	Zwykła prośba w toczącej się korespondencji, znana domena, brak linka i presji czasu
3	ATAK	Śmiesznie niska kwota to metoda, nie przypadek — ma zniechęcić do sprawdzania. Przewoźnicy nie pobierają dopłat SMS-em z linkiem
4	ATAK	Trzy sygnały naraz: presja, zakaz rozmowy przez telefon i prośba o poufność wobec zespołu. Prawdziwy prezes nie zabrania weryfikacji
5	ATAK — do czasu telefonu	Nawet jeżeli wiadomość jest prawdziwa, odpowiedź jest ta sama: dzwonisz na numer, który miałeś wcześniej , nie na ten z maila. To jest ten jeden przypadek, w którym „nie wiem” oznacza „nie płacę”
6	ATAK	Domena microsoft-alert365.com nie należy do Microsoftu. Żaden dostawca poczty nie prosi o „potwierdzenie obecnego hasła”
7	OK	Powiadomienie o zdarzeniu, bez linka i bez prośby o dane; odsyła do aplikacji i numeru z karty. Tak wygląda prawdziwa wiadomość z banku
8	ATAK	Straszy utratą twojej własnej pracy , nie karą — to najskuteczniejszy wariant. Subskrypcje sprawdzasz, logując się do narzędzia, nie z maila
9	OK	Własna domena firmy, wewnętrzny nadawca, brak presji i brak prośby o dane logowania. Warto tylko sprawdzić literówkę w domenie
10	ATAK	Faktura nigdy nie przychodzi jako archiwum ZIP . Archiwum jest po to, żeby ominąć skanowanie załącznika i żeby to odbiorca własnoręcznie uruchomił to, co jest w środku

Wynik zespołu

Poprawnych	Co to znaczy	Co robisz
9–10	Zespół rozpoznaje mechanizm, nie tylko przykłady	Powtórz test za pół roku na nowych wiadomościach
6–8	Oczywiste ataki wyłapane, te dopracowane — nie	Wdrażasz zasadę dwóch kanałów i dwuskładnikowe logowanie w tym tygodniu
0–5	Firma jest jedną wiadomością od straty	Pierwszy przelew powyżej progu, który sam ustalisz, wymaga akceptacji drugiej osoby. Od dziś, nie od szkolenia

Zwróć uwagę na coś innego niż liczba punktów: **kto zaznaczył ATAK przy wiadomościach 2, 7 i 9.**

Nadmiarowa podejrzliwość zatrzymuje normalną pracę firmy i po dwóch tygodniach zamienia się w klikanie we wszystko, bo „i tak wszystko jest podejrzane”. Celem nie jest strach. Celem jest jeden nawyk: **przy pieniądzach i przy haśle — drugi kanał.**

Trzy zdania do powieszenia po teście

1. **Zmiana numeru rachunku = telefon na numer, który mieliśmy wcześniej.** Zawsze, bez wyjątku dla stałych kontrahentów.
2. **Dokumenty pobieramy po zalogowaniu na platformę, nigdy z linka w wiadomości.**
3. **Faktura w archiwum ZIP nie jest fakturą.** Nie otwieramy, zgłaszamy.

Test opracował Daniel Kacprowicz na podstawie wiadomości, które realnie krążą po polskich firmach, oraz ostrzeżeń CERT Polska. Materiał jest bezpłatny — możesz go drukować i przeprowadzać u siebie bez pytania o zgodę. Incydent zgłaszasz na incydent.cert.pl albo przez mObywatel.szkolimy24.com · biuro@szkolimy24.com

Potrzebujesz z tym pomocy?

Prowadzę szkolenia dla instytucji publicznych z bezpieczeństwa pracy, cyberbezpieczeństwa i praktycznego wykorzystania sztucznej inteligencji. Jeżeli chcesz omówić wyniki albo szkolenie dla swojego zespołu — napisz przez formularz na stronie.

szkolimy24.com/procedura