



## Jak cyberprzestępcy wykorzystują Twoje emocje

### Kosztowna wiadomość SMS

Emma właśnie wyszła ze sklepu spożywczego, z ramionami pełnymi toreb, gdy jej telefon zabrzączał. Była to wiadomość SMS od córki.

***"Mamo, zgubiłam telefon! Piszę z telefonu przyjaciółki. Potrzebuję pieniędzy na nowy. Proszę prześlij mi 800 zł"***

Emmie serce zabiło szybciej. Jej córka Anna, wyjechała na studia i wiedziała, jak ważny jest dla niej telefon w szkole, pracy i utrzymywaniu kontaktu. Myśl o tym, że utknęła bez telefonu, sprawiła że poczuła niepokój. Odpisała,

***"Wszystko w porządku? Jak to się stało?"***

Odpowiedź przyszła niemal natychmiast.

***"Jest OK, ale nie mogę teraz rozmawiać. Pożyczyłam telefon od koleżanki. Czy możesz przesłać mi te pieniądze? Naprawdę ich potrzebuję. Zadzwoń wieczorem. Kocham Cię!"***

Emma zawahała się przez moment. Przeczynała, że coś było nie tak, ale nie zastanawiała się długo. Zalogowała się do aplikacji bankowej i zrobiła przelew na wskazanych w wiadomości numer konta. Nie zastanawiała się nawet, dlaczego nie robi przelewu na konto córki - być może Anna nie miała do nich dostępu bez swojego telefonu.

Późnym wieczorem zadzwoniła pod prawdziwy numer córki. Anna odebrała.

***"Cześć mama. Co tam?"***

Emma zesztywniała.

***"Otrzymałaś pieniądze?"***

Anna była zdezorientowana.

***"Jakie pieniądze?"***

Emma usiadła z wrażenia. Ponownie otworzyła poprzednie wiadomości tekstowe. Nagle dostrzegła to czego nie widziała wcześniej - nagły ton, brak konkretów, naleganie na natychmiastową płatność - **to oszustwo**. Oszust podawał się za jej córkę, wiedząc że spanikowana matka zrobi wszystko aby pomóc dziecku.

Niestety, nie tylko jej to dotknęło. Każdego dnia cyberprzestępcy manipulują emocjami, aby nakłonić ludzi do popełniania kosztownych błędów. Oto pięć typowych wyzwalaczy emocji. Sprawdź jak je wykryć zanim będzie za późno.

## 1. Pilność - „Działaj teraz albo coś stracisz”

Oszuści tworzą sztuczną presję czasu, aby zmusić użytkownika do popełnienia błędu.

**Jak to działa:**

***"Konto bankowe zostało przejęte! Potwierdź swoją tożsamość w ciągu godziny, w przeciwnym razie Twoje środki zostaną zablokowane."***

- „Twoja płatność została zaakceptowana", choć wiesz, że nie dokonywałeś żadnych zakupów.
- „Twoje hasło wkrótce wygaśnie! Zaktualizuj je natychmiast tutaj”.

**Jak to wykryć:**

- Skontaktuj się bezpośrednio z daną firmą, korzystając z danych kontaktowych podanych na oficjalnej stronie firmy lub korzystając z aplikacji mobilnej.
- Doszukuj się niejasnych szczegółów w wiadomości. Prawdziwe firmy piszą konkrety, a nie groźby.

## 2. Strach - „Wydarzy się coś złego”

Cyberprzestępcy wykorzystują strach, aby wywołać panikę i zmusić ofiary do działania bez zastanowienia.

**Jak to działa:**

- *"Urząd Skarbowy. Nie uregulowano zaległych podatków. Opłać je natychmiast, w przeciwnym razie sprawa zostanie przekazana do organów ścigania."*
- *„Urządzenie zostało zainfekowane! Zadzwoń pod ten numer, aby uzyskać wsparcie”.*
- *„Jeśli nie zapłacisz okupu, twoje prywatne zdjęcia zostaną opublikowane w sieci”.*

**Jak to wykryć:**

- Agencje rządowe nie grożą za pośrednictwem wiadomości tekstowych lub e-mail.
- Firmy antywirusowe nie skontaktują się z Tobą, aby ochronić urządzenie.

## 3. Ciekawość - „Nie uwierzysz w to!”

Oszuści wykorzystują ciekawość, używając szokujących lub kuszących wiadomości.

**Jak to działa:**

- *„Czy Ty jesteś na tym filmie? 😱” (ze złośliwym linkiem)*
- *„Wiadomość z ostatniej chwili! Ogromny skandal z udziałem celebryty - kliknij, aby zobaczyć”.*
- *„Twój przyjaciel oznaczył cię w szalonym poście!”.*

**Jak to wykryć:**

- Bądź sceptyczny wobec sensacyjnych wiadomości.
- Przed kliknięciem czegokolwiek lepiej skontaktuj się z nadawcą.

## 4. Zaufanie i autorytet - „To ktoś, kogo znasz”

Cyberprzestępcy podszywają się pod osoby, które znasz - członków rodziny, przyjaciół czy osoby z pracy.

**Jak to działa:**

- *"Cześć mama, to ja! Zgubiłam telefon. Czy możesz przelać mi pieniądze na nowy?"*
- *"Tu Twój szef. Zakup karty podarunkowe na imprezę biurową".*
- *„Wykryliśmy podejrzaną aktywność na Twoim koncie. Kliknij, aby zabezpieczyć je teraz”.*

**Jak to wykryć:**

- Ustal tajne hasło z członkami rodziny, aby wzajemnie weryfikować swoją tożsamość.
- Zwróć uwagę, że oszuści często nie znają Twojego imienia i nazwiska lub adresu korespondencyjnego.
- Uważaj na nietypowe żądania, zwłaszcza te dotyczące pieniędzy lub poufnych informacji.

## 5. Ekscytacja i chciwość - „Wygrałeś coś niesamowitego!”

Oszustwa typu „zbyt dobre, by mogło być prawdziwe” żerują na ludzkim pragnieniu nagrody lub uwagi.

**Jak to działa:**

- *"Gratulacje! Wygrałeś iPhone'a - odbierz go teraz!"*
- *„Wyglądasz wspaniale, powiedz mi coś więcej o sobie”.*
- *„Zostałeś wybrany do wyjątkowej okazji inwestycyjnej”.*

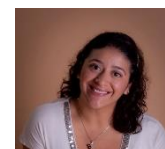
**Jak to wykryć:**

- Zasada jest prosta, skoro nie brałeś udziału w loterii, to nic nie wygrałeś. Legalne firmy nie wymagają opłaty za przesłanie nagrody.
- Uważaj na nieznajomych, którzy uparczywie wciskają coś, co jest „zbyt piękne, by mogło być prawdziwe” lub zbyt szybko wyrażają romantyczne uczucia.
- Bądź również sceptyczny wobec „ekskluzywnych” ofert wysyłanych losowo.

Następnym razem, gdy otrzymasz pilną wiadomość tekstową lub telefoniczną, zatrzymaj się, pomyśl i zweryfikuj, zanim podejmiesz działanie. Nie pozwól, aby emocje wzięły górę!

### Redaktor gościnny

Teressa Gehrke jest założycielką [PopCykol](#), firmy zajmującej się bezpieczeństwem online. Ma ponad 10-letnie doświadczenie w branży konsultingowej jako osoba techniczna, projektant UX i kierownik projektu. Jest członkiem zarządu WiCyS Colorado. Teressa jest również muzykiem. [Linktree](#)



## Źródła

**Miła rozmowa i pusty portfel: Oszustwa romantyczne:** <https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/>

**Ataki z wykorzystaniem odwzorowanego głosu:** <https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/>

**Ataki za pomocą wiadomości tekstowych:** <https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/>

### Polski przekład CERT Polska: Aleksandra Węgrzynowicz, Bartłomiej Wnuk

OUCH! OUCH! jest publikowany przez firmę SANS Security Awareness i jest rozpowszechniany pod licencją [Creative Commons BY-NC-ND 4.0 license](#). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszenia zawartości samego biuletynu. Zespół redakcyjny: Phil Hoffman, Leslie Ridout, Princess Young.