

CYBERBEZPIECZEŃSTWO POSTAWY I ZACHOWANIA POLAKÓW



Raport | Część I | Cyberbezpieczeństwo
w internecie

Październik 2026

SPIS TREŚCI

WSTĘP	3
AKTYWNOŚĆ POLAKÓW W INTERNECIE	5
POCZUCIE BEZPIECZEŃSTWA W INTERNECIE	7
ŚWIADOMOŚĆ ZAGROŻEŃ	8
METODY OCHRONY A NIEOSTROŻNE NAWYKI	12
DOŚWIADCZENIA OSZUSTWA LUB CYBERATAKU	21
ZAKOŃCZENIE	30

O BADANIU

Badanie zrealizowane przy współpracy z firmą IQS, metodą CAWI na panelu Opinie.pl.
Próba reprezentatywna dla populacji (N = 1000), osoby bankujące w wieku 18-70 lat.

Pokolenia: Gen Z (18-29 lat), N = 248; Gen Y (30-44 lata), N = 248; Gen X (45-60 lat),
N = 252; Baby Boomers (>60 lat), N = 252.

Na wykresach odpowiedzi „Tak” i „Nie” odpowiadają sumie pozytywnych („zdecydowanie”
i „raczej się zgadzam”) oraz negatywnych („zdecydowanie” i „raczej się nie zgadzam”) ocen
na 5-stopniowej skali Likerta wykorzystanej w badaniu.

WSTĘP

Cyfrowe rozwiązania stały się fundamentem codzienności Polaków. Smartfon już dawno przestał być jedynie narzędziem komunikacji – dziś to osobisty asystent, portfel i brama do świata usług finansowych. Z poziomu aplikacji mobilnej kontrolujemy swoje finanse, wykonujemy przelewy, opłacamy rachunki czy inwestujemy. A w e-commerce coraz częściej wybieramy płatności kartą online, oczekując, że zakup będzie szybki, intuicyjny i w pełni bezpieczny.

Razem z Mastercard przyglądamy się temu, jak Polacy funkcjonują w tej rzeczywistości finansowej. Chcemy lepiej zrozumieć, z jakich rozwiązań korzystają najczęściej, jak postrzegają bezpieczeństwo cyfrowe oraz jakie mają doświadczenia związane z bankowością mobilną i płatnościami kartowymi w internecie. To szczególnie ważne, bo choć technologie oferują coraz bardziej zaawansowane zabezpieczenia, krajobraz zagrożeń zmienia się równie dynamicznie.

Dzisiejsi cyberprzestępcy sięgają po nowoczesne narzędzia i metody manipulacji. Fałszywe bramki płatności, podszywanie się pod znane marki, wyłudzenie danych przez fałszywe wiadomości i strony internetowe, oszustwa za pośrednictwem SMS-ów czy przejmowanie kont to tylko część zagrożeń, z którymi każdy z nas może zetknąć się na co dzień. Jednocześnie rośnie świadomość Polaków: coraz lepiej rozpoznajemy podejrzane komunikaty, zwracamy uwagę na ustawienia bezpieczeństwa w aplikacjach, ostrożniej podajemy dane kartowe i bardziej świadomie korzystamy z technologii mobilnych.

Celem raportu „Cyberbezpieczeństwo – postawy i zachowania Polaków” jest pokazanie, jak wygląda równowaga między wygodą a bezpieczeństwem. Raport składa się z dwóch części: „Cyberbezpieczeństwo w internecie” oraz „Cyberbezpieczeństwo w bankowości internetowej i mobilnej”. W pierwszej części, którą prezentujemy obecnie, przyglądamy się

aktywności Polaków w internecie, ich poczuciu bezpieczeństwa i świadomości zagrożeń, a także stosowanym metodom ochrony, nieostrożnym nawykom oraz doświadczeniom związanym z oszustwami i cyberatakami.

Choć instytucje finansowe stosują zaawansowane mechanizmy ochrony, kluczową rolę nadal odgrywają codzienne zachowania użytkowników: sposób logowania, czujność wobec podejrzanych wiadomości, dbałość o dane i świadome korzystanie z karty podczas zakupów w sieci.

Wierzymy, że nowoczesna bankowość może być jednocześnie wygodna i bezpieczna. Ten raport to krok w stronę lepszego zrozumienia potrzeb, obaw i nawyków Polaków – po to, aby wspólnie tworzyć środowisko finansowe, które będzie przyjazne, intuicyjne i odporne na zagrożenia cyfrowe.

Michał Nagórka, Dyrektor Centrum Bezpieczeństwa Banku

Bartosz Zborowski, Dyrektor Departamentu Zintegrowanych Kanałów i Sprzedaży Cyfrowej
Jorge Sánchez, Dyrektor Departamentu Marketingu

SMARTFON STAŁ SIĘ NASZYM CODZIENNYM „CENTRUM DOWODZENIA”

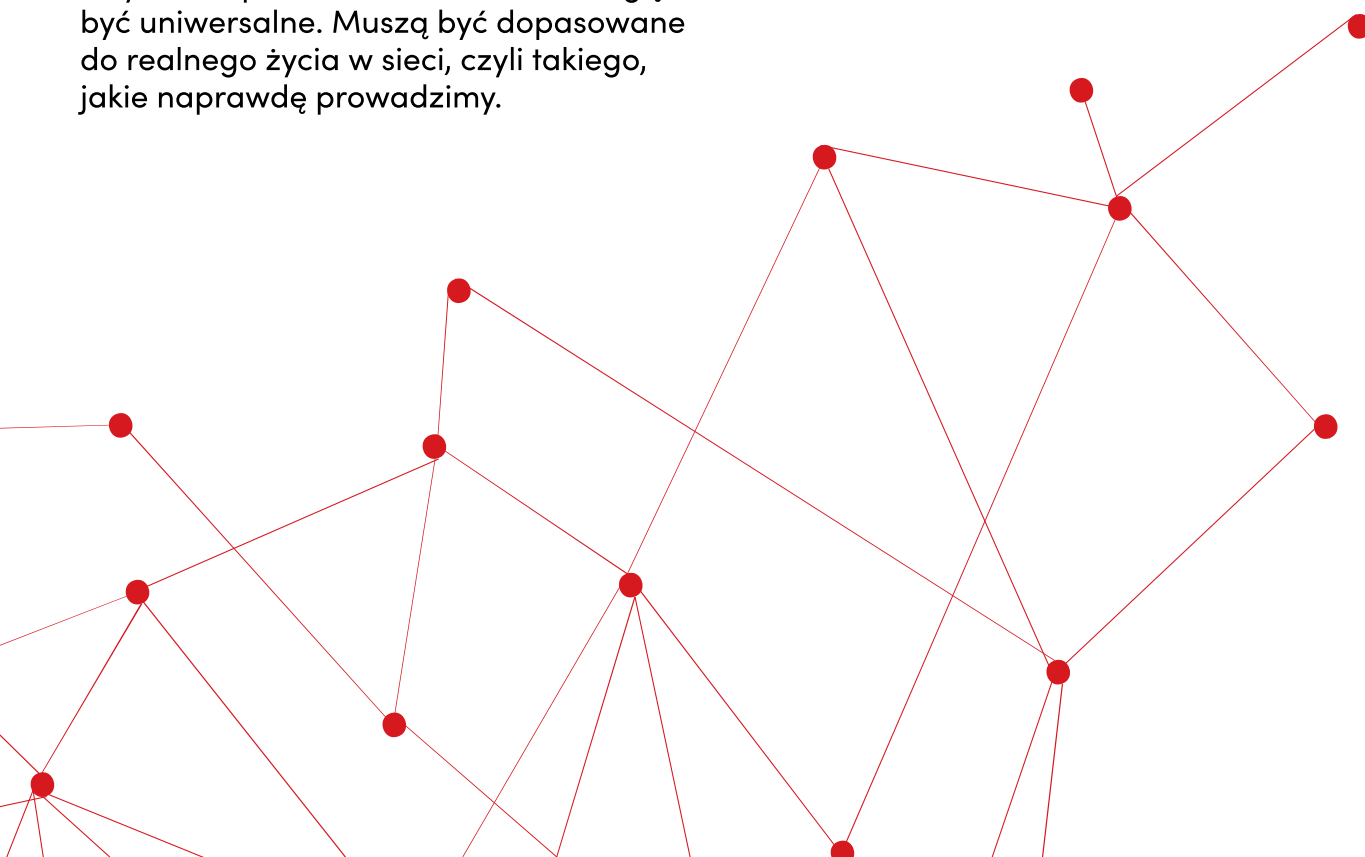
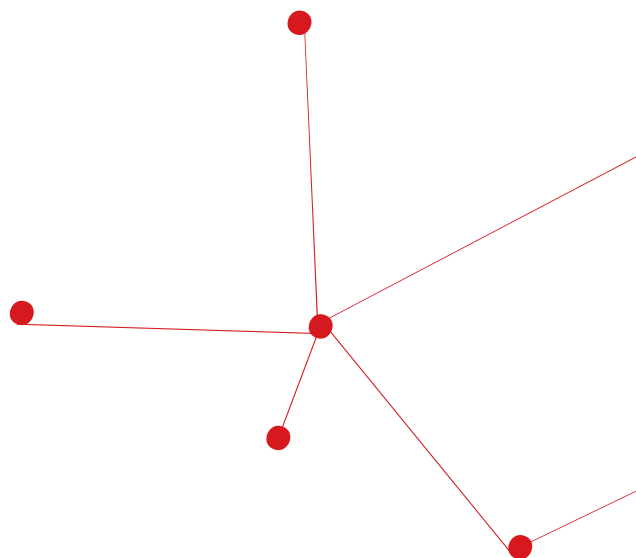
Smartfon daje nam wygodę, szybkość i dostęp do wszystkiego w jednym miejscu.

Ale wraz z tą wygodą pojawiają się też nowe ryzyka. Oszuści doskonale wiedzą, że działamy w biegu, często z przyzwyczajenia i bez chwili zastanowienia i stale próbują wykorzystać tę wiedzę, żeby dostać się do naszych danych lub pieniędzy. Dlatego dziś o bezpieczeństwie decyduje nie tylko technologia, ale przede wszystkim to, jak korzystamy z internetu na co dzień.

Aby lepiej zrozumieć obawy związane z cyberbezpieczeństwem, warto najpierw przyjrzeć się codziennym praktykom i zachowaniom użytkowników.

Ile czasu spędzamy w sieci, z jakich urządzeń korzystamy, do czego najczęściej używamy internetu? I co także ważne, czy te nawyki różnią się między pokoleniami?

To właśnie ten kontekst pozwala lepiej zrozumieć cały raport. Pokazuje, że nie ma jednego „typowego użytkownika” internetu, ale są różne style korzystania z sieci, różne potrzeby i wreszcie różne poziomy doświadczenia. A to oznacza, że skuteczna edukacja i komunikacja o cyberbezpieczeństwie także nie mogą być uniwersalne. Muszą być dopasowane do realnego życia w sieci, czyli takiego, jakie naprawdę prowadzimy.



BANKOWOŚĆ, ZAKUPY I SOCIAL MEDIA NALEŻĄ DO CODZIENNYCH AKTYWNOŚCI CYFROWYCH WIĘKSZOŚCI POLAKÓW

84%KORZYSTA
Z BANKOWOŚCI ONLINE**44%**

KORZYSTA RAZ DZIENNIE LUB CZĘŚCIEJ

83% **29%** **80%**ROBI ZAKUPY
ONLINE**69%** **61%**

2-3 RAZY W MIESIĄCU LUB CZĘŚCIEJ

41% **77%**KORZYSTA Z MEDIÓW
SPOŁECZNOŚCIOWYCH**69%**

KORZYSTA RAZ DZIENNIE LUB CZĘŚCIEJ

89% **23%** 

Usługi cyfrowe stały się nieodłącznym elementem codziennego życia Polaków. Z bankowości internetowej korzysta 84% użytkowników, 80% robi zakupy online, a 77% aktywnie używa mediów społecznościowych. Co ważne, większość z tych aktywności realizowana jest regularnie. We wszystkich obszarach dominującym urządzeniem jest

smartfon, z którego korzysta od 69% do 89% użytkowników. Potwierdza to mobilny charakter aktywności online i pokazuje, że kanały cyfrowe są dziś podstawowym środowiskiem, w którym użytkownicy zarządzają swoimi finansami, komunikują się, dokonują zakupów i realizują codzienne potrzeby.

INTERNET JEST WSPÓLNĄ PRZESTRZENIĄ WSZYSTKICH GENERACJI

GEN Z (18–29 lat)

Główne aktywności:

89% E-mail

86% Media społecznościowe

79% Zakupy

78% Bankowość internetowa/mobilna

GEN Y (30–44 lat)

Główne aktywności:

88% E-mail

85% Bankowość internetowa/mobilna

82% Media społecznościowe

82% Zakupy

GEN X (45–60 lat)

Główne aktywności:

92% E-mail

87% Bankowość internetowa/mobilna

82% Zakupy

73% Media społecznościowe

BABY BOOMERS (BB)

(60 lat i więcej)

Główne aktywności:

93% E-mail

84% Bankowość internetowa/mobilna

78% Zakupy

69% Media społecznościowe

DZIENNY CZAS SPĘDZONY ONLINE – PERSPEKTYWA POKOLENIOWA

5 h 13 m

Z

3 h 59 m

Y

3 h 54 m

X

3 h 24 m

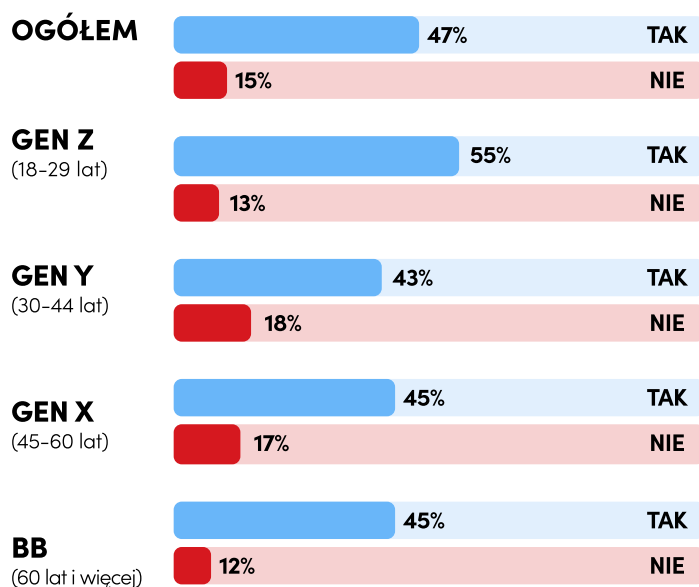
BB

Cyfrowi liderzy, czyli generacja Z, spędza online ponad 5 godzin dziennie, podczas gdy starsze grupy poświęcają na aktywności cyfrowe mniej czasu. Niezależnie od wieku Polacy najczęściej korzystają z poczty e-mail, robią zakupy online, używają mediów społecznościowych i komunikatorów oraz korzystają z bankowości internetowej,

która należy do najpowszechniejszych aktywności cyfrowych (78–87%). Różnice między pokoleniami dotyczą przede wszystkim sposobu integracji internetu z codziennym życiem, a nie samej obecności w kanałach cyfrowych.

CYBERZAGROŻENIA SĄ REALNE NAWET DLA TYCH, KTÓRZY CZUJĄ SIĘ BEZPIECZNIE

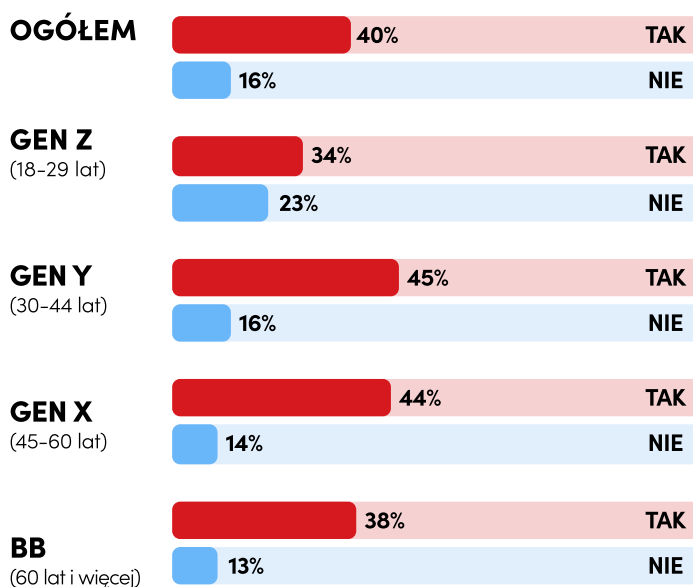
Czy czujesz się bezpiecznie w internecie?



POZYTYWNE POSTRZEGANIE BEZPIECZEŃSTWA ONLINE PRZEWAŻA NAD POCZUCIEM ZAGROŻENIA.

Niemal połowa Polaków (47%) deklaruje, że czuje się bezpiecznie w internecie, przy czym wskaźnik ten jest najwyższy wśród najmłodszych użytkowników (55% w grupie 18–29 lat). Jednocześnie tylko niewielki odsetek respondentów wyraźnie odczuwa brak bezpieczeństwa w internecie (15%), co sugeruje przewagę pozytywnych odczuć wobec świata cyfrowego.

Czy uważasz, że możesz paść ofiarą cyberataku?



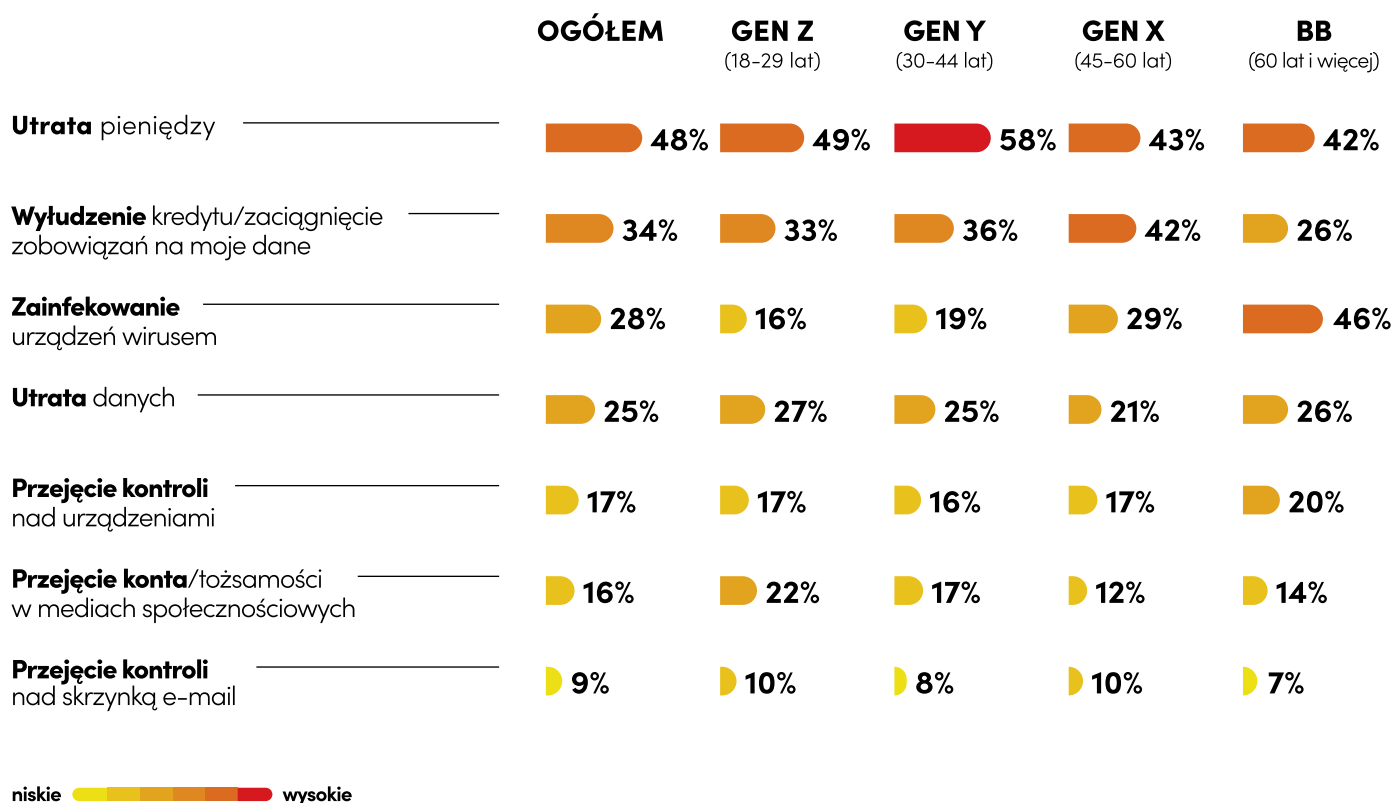
ŚWIADOMOŚĆ RYZYKA CYBERATAKÓW JEST WYRAŻNA.

Czterech na dziesięciu uczestników badania (40%) uważa, że może stać się ofiarą cyberataku, a przekonanie to jest szczególnie silne wśród osób w wieku 30–44 lata (45%). Jednocześnie jedynie 16% badanych wyklucza taką możliwość, co pokazuje, że większość użytkowników postrzega cyberzagrożenia jako realne i dotyczące również ich samych.

Na uwagę zwraca również znacząca grupa osób, które nie potrafią ocenić własnej podatności na cyberzagrożenia. Może to wskazywać na brak świadomości w tym obszarze i potencjalnie zwiększone ryzyko w tej grupie.

CYBERATAKI KOJARZĄ SIĘ PRZED W SZYSTKIM Z UTRATĄ PIENIĘDZY

OBAWY ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM



WYRÓŻNIKI POKOLEŃ

Z Największą obawą Pokolenia Z jest utrata pieniędzy, ale na tle innych pokoleń wyróżnia je wyższy lęk przed przejęciem konta w mediach społecznościowych.

X Pokolenie X częściej niż pozostałe pokolenia obawia się wyłudzenia kredytu lub zaciągnięcia zobowiązań na swoje dane.

Y Pokolenie Y najsilniej spośród wszystkich grup obawia się utraty pieniędzy.

BB Wśród Baby Boomers szczególnie silna jest obawa przed zainfekowaniem urządzenia wirusem.

OBAWY ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM MAJĄ PRZED WSZYSTKIM WYMIAR FINANSOWY

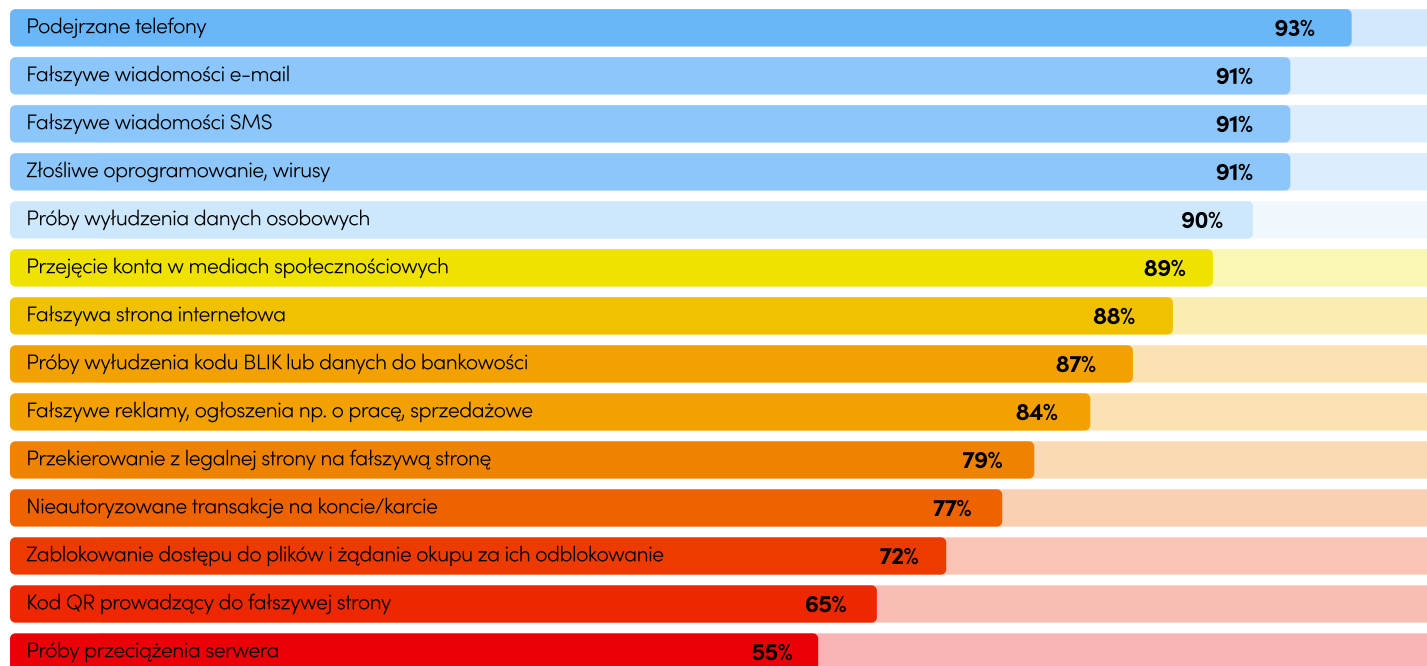
Najczęściej wskazywaną obawą jest utrata pieniędzy (48%), a następnie wyłudzenie kredytów lub innych zobowiązań na skradzione dane osobowe (34%). Wyniki pokazują, że zagrożenia bezpośrednio wpływające na sytuację materialną są postrzegane jako najbardziej dotkliwe i najbardziej realne.

ZAGROŻENIA TECHNICZNE BUDZĄ WYRAŹNIE MNIJSZE OBAWY NIŻ RYZYKA FINANSOWE

Spośród nich najczęściej wskazywane są zainfekowanie urządzenia wirusem (28%) oraz utrata danych (25%), podczas gdy przejęcie kontroli nad urządzeniem (17%), kontami internetowymi lub społecznościowymi (16%) czy skrzynką e-mail (9%) jest wymieniane znacznie rzadziej. Może to świadczyć o tym, że tego typu zagrożenia są postrzegane jako mniej dotkliwe lub mniej prawdopodobne niż te prowadzące do bezpośrednich strat finansowych.

NAJWIĘKSZA ŚWIADOMOŚĆ TYLKO PROSTYCH ZAGROŻEŃ

ZNAJOMOŚĆ ZAGROŻEŃ W SIECI



WYRÓŻNIKI POKOLEŃ

Z Pokolenie Z najczęściej na tle innych pokoleń (91%) rozpoznaje próby wyłudzenia kodu BLIK i danych do bankowości.

BB Znajomość oszustw związanych z BLIK-iem i mediami społecznościowymi jest najniższa wśród Baby Boomers (79% i 84%).

ŚWIADOMOŚĆ NAJPOPULARNIEJSZYCH CYBERZAGROŹEŃ JEST POWSZECHNA I OBEJMUJE ZDECYDOWANĄ WIĘKSZOŚĆ POLAKÓW

Najlepiej rozpoznawane są zagrożenia, z którymi użytkownicy stykają się najczęściej w mediach i codziennym korzystaniu z internetu, czyli podejrzane telefony (93%), fałszywe wiadomości e-mail i SMS (po 91%), złośliwe oprogramowanie (91%), próby wyłudzenia danych osobowych (90%) czy przejęcia kont w mediach społecznościowych (89%). Nieco niższa, choć nadal bardzo wysoka, jest znajomość bardziej złożonych schematów oszustw, takich jak fałszywe strony internetowe (88%) oraz wyłudzenia kodów BLIK (87%).

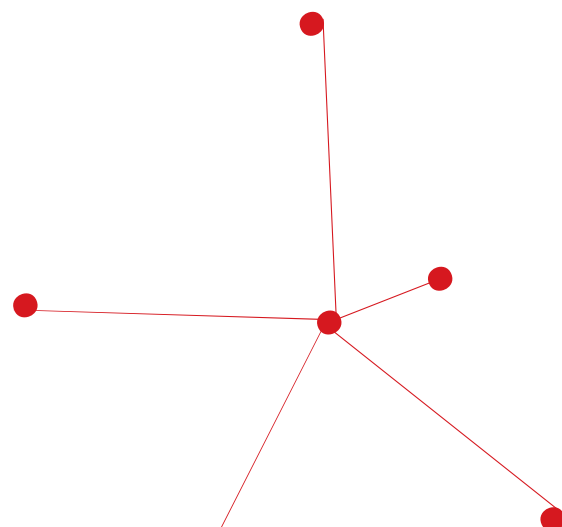
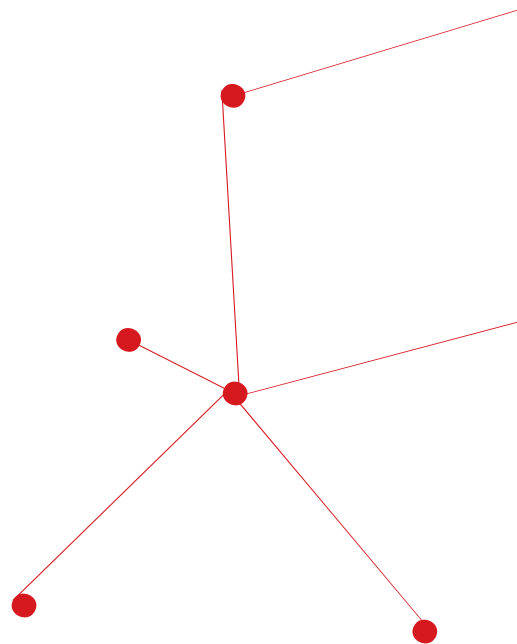
MNIEJ ROZPOZNAWALNE SĄ BARDZIEJ ZŁOŻONE I TECHNICZNE CYBERZAGROŻENIA

Choć większość respondentów zna podstawowe ryzyka, poziom świadomości spada w przypadku mniej oczywistych form ataków. 79% respondentów wie o przekierowaniach na fałszywe strony internetowe, a 65% rozpoznaje zagrożenia związane z fałszywymi stronami ukrytymi pod kodami QR. Najniższą znajomość odnotowano w przypadku ataków polegających na przeciążaniu serwerów, które zna jedynie 55% badanych.

Świadomość cyberzagrożeń jest szeroka, ale nierównomierna. Najwyższa w przypadku najczęstszych i najbardziej nagłaśnianych oszustw, a wyraźnie niższa tam, gdzie zagrożenia są bardziej złożone lub mniej widoczne w codziennym doświadczeniu użytkowników.

ZNANE PODSTAWY I NOWE PUŁAPKI W SIECI

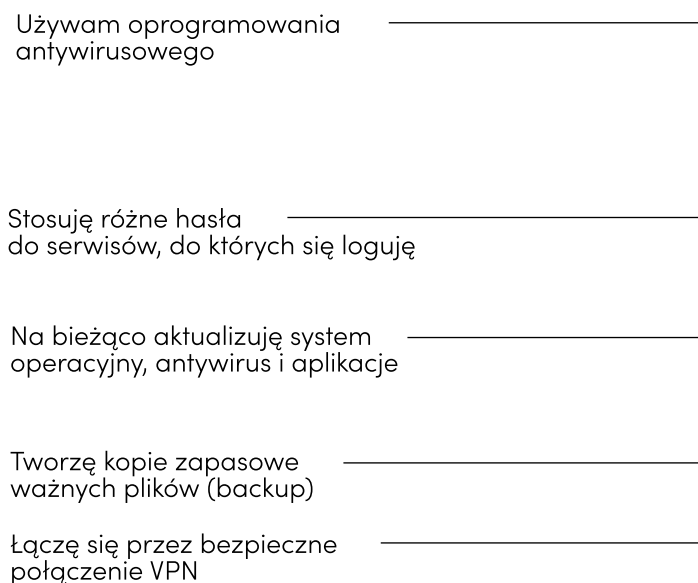
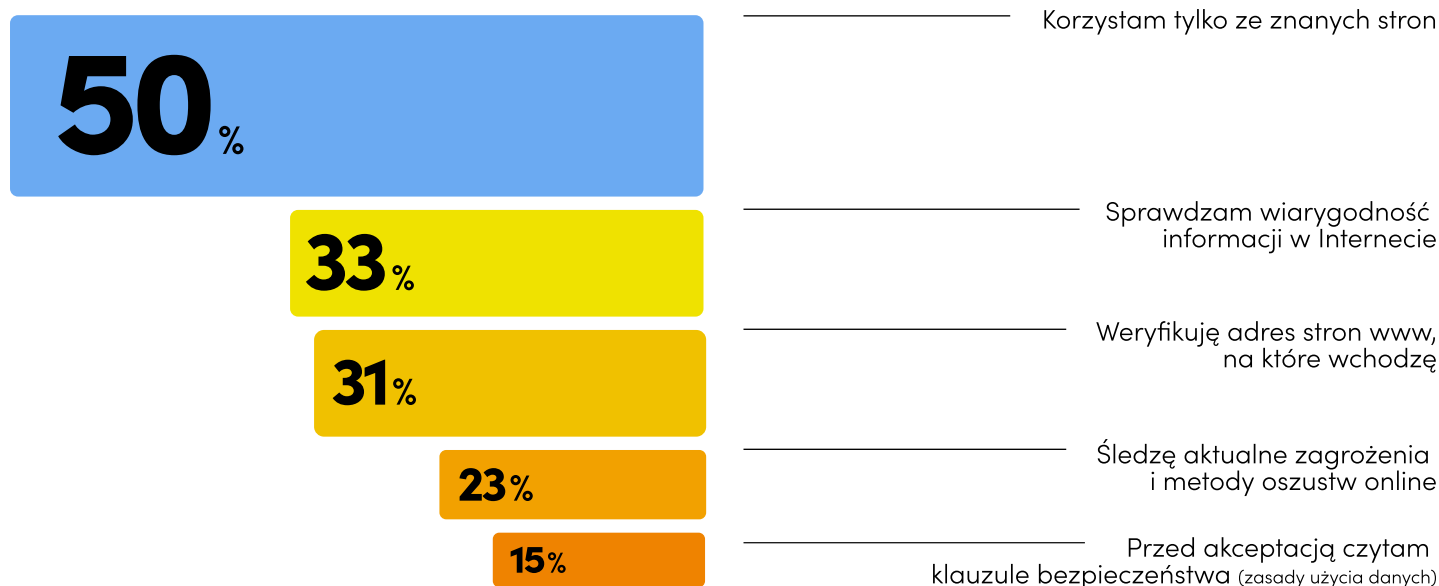
Całość pokazuje, że Polacy w dużym stopniu orientują się w katalogu zagrożeń, jednak istnieje przestrzeń do wzmacniania wiedzy w obszarach mniej oczywistych, które często stanowią rosnące pole aktywności cyberprzestępców.



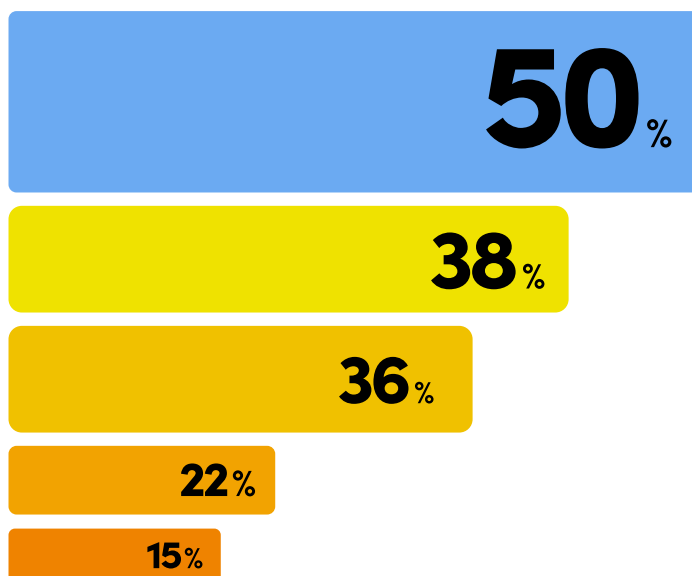
OSTROŻNOŚĆ PRZED TECHNOLOGIĄ, CZYLI OCHRONA W SIECI

PODEJMOWANE DZIAŁANIA ZWIĘKSZAJĄCE BEZPIECZEŃSTWO W INTERNECIE

OSTROŻNOŚĆ I HIGIENA PRZEGLĄDANIA



OCHRONA DANYCH I URZĄDZEŃ



BEZPIECZEŃSTWO STOI NA ANTYWIRUSIE I ZNANYCH STRONACH

Najczęściej stosowane działania zwiększające bezpieczeństwo w internecie to korzystanie wyłącznie ze znanych stron internetowych oraz używanie oprogramowania antywirusowego (50%).

Rzadziej respondenci deklarowali używanie różnych haseł do serwisów, do których się logują (38%) oraz regularne aktualizowanie systemu operacyjnego, oprogramowania antywirusowego i aplikacji (36%). Około jedna trzecia sprawdza wiarygodność informacji w internecie (33%) lub weryfikuje adres stron, na które wchodzi (31%).

Tworzenie kopii zapasowych danych (22%) czy śledzenie aktualnych zagrożeń (23%) pozostają działaniami stosunkowo rzadkimi. Jeszcze mniej osób korzysta z bezpiecznych połączeń VPN (15%).

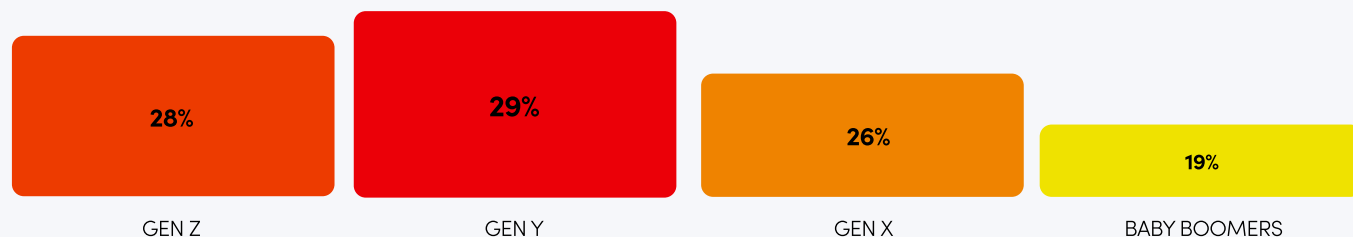
DEKLARUJEMY OSTROŻNOŚĆ, ALE RYZYKO WCIAŻ ISTNIEJE

KLIKANIE W OTRZYMANE LINKI BEZ ICH SPRAWDZENIA

25%

KLIKA W NIESPRAWDZONE LINKI

Podział na poszczególne generacje



68%

NIGDY NIE KLIKA W LINK
BEZ WCZEŚNIEJSZEGO SPRAWDZENIA

WPISYWANIE DANYCH KARTY PŁATNICZEJ NA NIE SWOIM URZĄDZENIU

19%

WPISUJE DANE KARTY NA OBCYM URZĄDZENIU

Podział na poszczególne generacje



75%

NIGDY NIE WPISUJE DANYCH KARTY PŁATNICZEJ
NA OBCYM URZĄDZENIU

LOGOWANIE SIĘ DO SERWISU INTERNETOWEGO BANKU BEZ SPRAWDZENIA ADRESU STRONY WWW

20%

LOGUJE SIĘ DO BANKU BEZ SPRAWDZENIA ADRESU STRONY

Podział na poszczególne generacje



70%

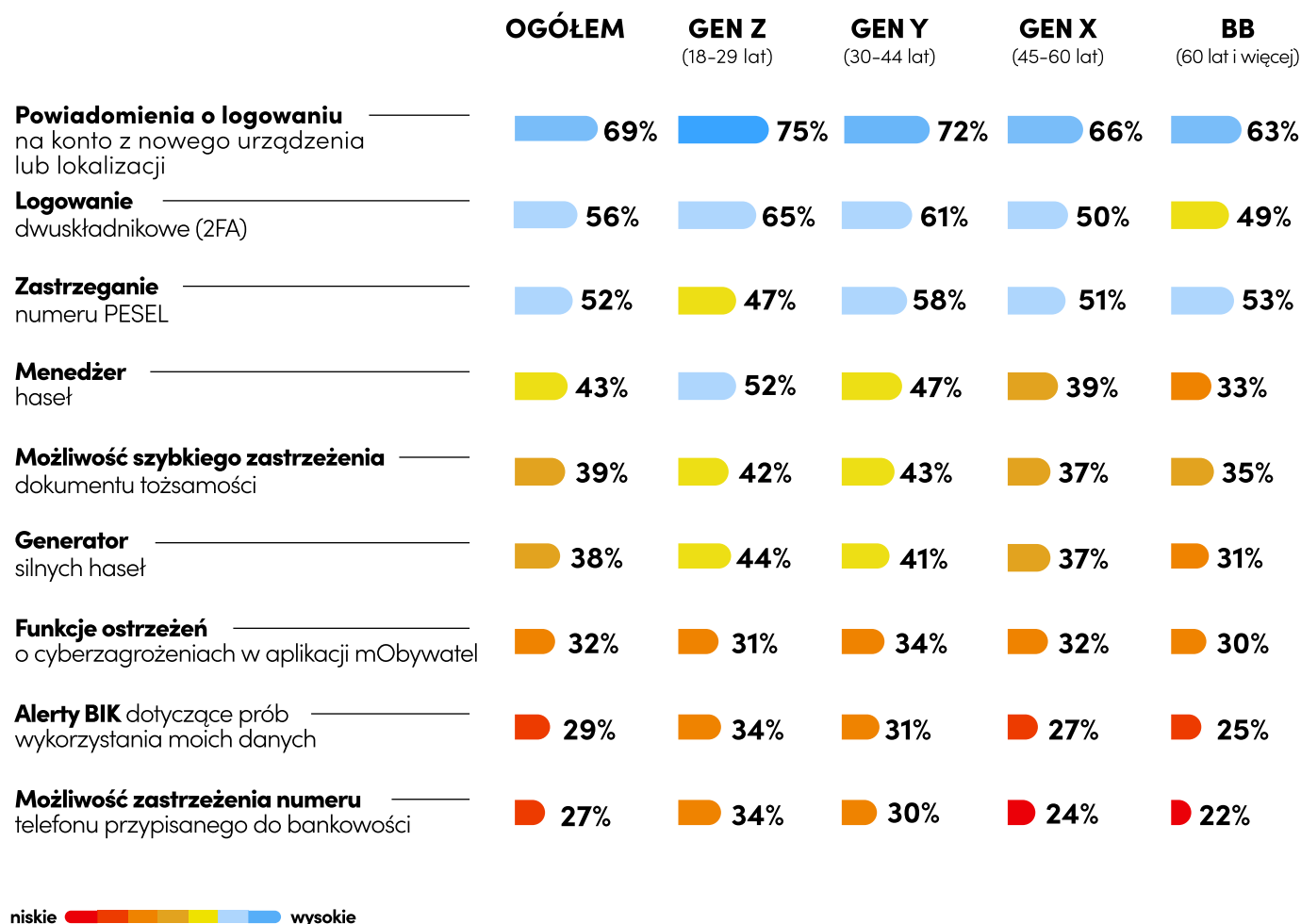
NIGDY NIE LOGUJE SIĘ DO BANKU BEZ SPRAWDZENIA ADRESU STRONY

Podstawowe zasady cyberbezpieczeństwa są znane i stosowane przez większość użytkowników. Od 68% do 75% respondentów deklaruje, że przed logowaniem weryfikuje adres strony banku, unika podejrzanych linków oraz nie podaje danych karty na cudzych urządzeniach. Wyniki pokazują jednak, że bezpieczne nawyki nie są jeszcze standardem dla wszystkich.

Młodsze grupy częściej podejmują działania, które mogą zwiększać podatność na cyberataki. To pokazuje, że kluczowym wyzwaniem pozostaje nie dalsze zwiększanie świadomości zagrożeń, ale budowanie trwałych nawyków bezpiecznego korzystania z usług cyfrowych.

PODSTAWOWE ZABEZPIECZENIA STANDARDEM CYBEROCHRONY

KORZYSTANIE Z NARZĘDZI WSPIERAJĄCYCH BEZPIECZEŃSTWO W INTERNECIE



WYRÓŻNIKI POKOLEŃ

Z Najmłodsze pokolenie najczęściej korzysta z narzędzi zwiększających bezpieczeństwo, szczególnie z powiadomień o logowaniu, logowania dwuetapowego oraz menedżerów i generatorów haseł.

X Przedstawiciele Pokolenia X rzadziej korzystają z logowania dwuskładnikowego.

Y Pokolenie Y częściej korzysta z możliwości szybkiego zastrzeżenia dokumentu tożsamości oraz numeru PESEL.

BB Baby Boomers rzadziej niż młodsze pokolenia korzystają z dodatkowych zabezpieczeń, szczególnie z menedżerów i generatorów haseł, logowania dwuskładnikowego czy powiadomień o logowaniu z nowego urządzenia lub lokalizacji.

NAJCZĘTNIEJ KORZYSTAMY Z ROZWIĄZAŃ, KTÓRE SĄ PROSTE, AUTOMATYCZNE I WBUDOWANE W CODZIENNE KORZYSTANIE Z USŁUG

Najczęściej stosowane są powiadomienia o logowaniu (69%) oraz uwierzytelnianie dwuskładnikowe (56%).

PO NARZĘDZIA WYMAGAJĄCE DODATKOWEGO ZAANGAŻOWANIA SIĘGA MNIJ UŻYTKOWNIKÓW

Rzadziej wykorzystywane są funkcje związane z monitorowaniem bezpieczeństwa i reagowaniem na incydenty, które wymagają świadomego działania użytkownika, tj. zastrzeżenia numeru PESEL (52%), alerty BIK (29%) czy zastrzeganie numeru telefonu przypisanego do bankowości elektronicznej (27%).

Menedżer haseł wykorzystuje 43% badanych, a generator silnych haseł 38%, co pokazuje, że wraz ze wzrostem wysiłku potrzebnego do korzystania z zabezpieczeń maleje ich popularność.

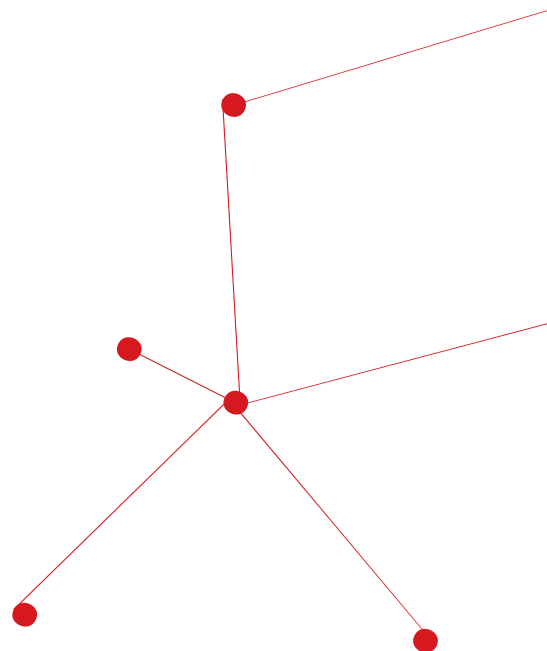
ŚWIADOMOŚĆ CYBERZAGROŹEŃ JEST WYSOKA, ALE NIE PRZEKŁADA SIĘ NA BEZPIECZNE NAWYKI I REALNE DZIAŁANIA OCHRONNE

Nadal duża część użytkowników nie korzysta z dodatkowych zabezpieczeń, mimo że to one w największym stopniu chronią przed przejęciem kont czy utratą danych.

Wciąż powszechne są ryzykowne nawyki: brak logowania wieloskładnikowego, stosowanie tych samych haseł w wielu serwisach, niekorzystanie z menedżerów haseł, nieweryfikowanie adresów stron przed logowaniem. To pokazuje, że teoretyczna wiedza nie jest jeszcze zamieniana na realne, codzienne praktyki bezpieczeństwa.

Alarmujące jest to, że co czwarty respondent przyznaje się do klikania w link bez uprzedniej weryfikacji, a niemal co piąty podaje dane karty płatniczej na urządzeniu, którego nie kontroluje. Te zachowania znacząco zwiększają ryzyko kradzieży danych, infekcji złośliwym oprogramowaniem czy utraty środków finansowych.

Cyberprzestępcy bazują właśnie na pośpiechu i braku czujności użytkowników, dlatego edukacja cyfrowa i budowanie nawyków ostrożnościowych są dziś równie ważne, jak stosowanie zaawansowanych narzędzi bezpieczeństwa.





Użytkownicy internetu deklarują znajomość zagrożeń oraz stosowanie podstawowych zabezpieczeń, jednak w praktyce poziom tej ochrony jest niewystarczający wobec dynamicznie ewoluujących technik cyberprzestępców.

Powiadomienia o logowaniu z nowego urządzenia stały się dziś standardem, ale mają one charakter przede wszystkim reaktywny – informują o potencjalnym incydencie dopiero wtedy, gdy próba przejęcia dostępu już nastąpiła. To oznacza, że użytkownik jest włączany w proces obrony w momencie, gdy ryzyko jest już wysokie. Równocześnie obserwujemy wciąż zbyt niski poziom wykorzystania mechanizmów, które rzeczywiście ograniczają skuteczność ataków. Logowanie dwuskładnikowe, silne uwierzytelnianie czy zaawansowane mechanizmy ochrony tożsamości nadal nie są stosowane konsekwentnie, zwłaszcza tam, gdzie mają największe znaczenie, czyli przy dostępie do usług finansowych i wrażliwych danych. W efekcie scenariusze takie jak przejęcie konta, phishing czy oszustwa wykorzystujące socjotechnikę pozostają relatywnie łatwe do przeprowadzenia, ponieważ atakujący nadal bazują na najłagodniejszym ogniwie – użytkowniku i jego nawykach.

Kluczowym wyzwaniem nie jest dziś brak technologii. Rynek oferuje szeroki wachlarz rozwiązań, które skutecznie podnoszą poziom bezpieczeństwa, od uwierzytelniania wieloskładnikowego, przez analizę behawioralną, po mechanizmy *risk-based authentication*. Problem leży w ich niesystematycznym wykorzystywaniu oraz niedostatecznym osadzeniu w codziennych procesach użytkowników i organizacji. W wielu przypadkach bezpieczeństwo wciąż traktowane jest jako dodatek, a nie integralny element doświadczenia użytkownika i architektury usług.

Z punktu widzenia bezpieczeństwa konieczna jest zmiana podejścia – przesunięcie ciężaru z wykrywania incydentów na zapobieganie im. Oznacza to wdrażanie takich mechanizmów, które nie tylko informują o zagrożeniu, ale realnie uniemożliwiają atak na etapie próby dostępu. Równie istotne jest budowanie trwałych nawyków użytkowników, tak aby korzystanie z silnych metod uwierzytelniania czy świadome zarządzanie tożsamością cyfrową były standardem, a nie wyjątkiem. Dopiero połączenie technologii z konsekwentnym jej stosowaniem oraz edukacją użytkowników pozwala realnie ograniczyć skalę cyberoszustw. W praktyce oznacza to przejście od modelu „wiemy, że trzeba się chronić” do modelu „chronimy się skutecznie, bo mamy właściwe mechanizmy i faktycznie z nich korzystamy”.



Robert Mazur,
Dyrektor Departamentu Cyberbezpieczeństwa

ŚWIADOMOŚĆ ZAGROZEŃ

ZABEZPIECZENIA W INTERNECIE – ZNAJOMOŚĆ A KORZYSTANIE

ZNAJOMOŚĆ

(zna, ale nie korzysta)

BARIERY KORZYSTANIA

47%

GENERATOR
SILNYCH HASEŁ

18% NIE MAM ZAUFANIA DO TEGO SPOSOBU

30% NIE JEST MI TO POTRZEBNE

16% OBAWIAM SIĘ, ŻE COŚ PRZYPADKOWO ZABLOKUJĘ

44%

SZYBKIE ZASTRZEŻENIE
TOŻSAMOŚCI

21% NIE WIEM, JAK TO WŁĄCZYĆ

36% NIE JEST MI TO POTRZEBNE

15% ZAPOMINAM O ICH STOSOWANIU

42%

MENEDŻER
HASEŁ

22% NIE MAM ZAUFANIA DO TEGO SPOSOBU

26% NIE JEST MI TO POTRZEBNE

13% ZAPOMINAM O ICH STOSOWANIU

39%

ZASTRZEGANIE NUMERU
PESEL

18% OBAWIAM SIĘ, ŻE COŚ PRZYPADKOWO ZABLOKUJĘ

44% NIE JEST MI TO POTRZEBNE

13% ZAPOMINAM O ICH STOSOWANIU

ZNAJOMOŚĆ

(zna, ale nie korzysta)

BARIERY KORZYSTANIA

27%

LOGOWANIE
DWUSKŁADNIKOWE

25% ZAJMUJE ZBYT DUŻO CZASU

17%

NIE JEST MI TO POTRZEBNE

17% TO ZBYT SKOMPLIKOWANE

20%

POWIADOMIENIA O LOGOWANIU
Z NOWEGO URZĄDZENIA LUB LOKALIZACJI

20% ZAPOMINAM O ICH STOSOWANIU

27%

NIE JEST MI TO POTRZEBNE

16% NIE WIEM, JAK TO WŁĄCZYĆ

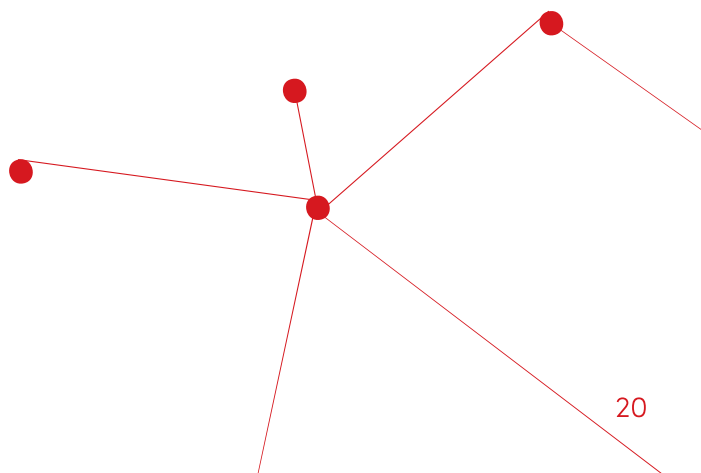
Baza: osoby, które znają narzędzie, ale z niego nie korzystają

Niskie wykorzystanie dodatkowych zabezpieczeń, pomimo ich znajomości, wskazuje, że upowszechnienie części rozwiązań nadal napotyka istotne bariery. Najczęstszą z nich jest brak odczuwanej potrzeby korzystania z tego typu narzędzi, wzmacniany przez złudne poczucie bezpieczeństwa i przekonanie, że „mnie to nie dotyczy”.

Jest to zarazem jedna z najtrudniejszych do przełamania postaw, ponieważ wynika nie tyle z braku możliwości korzystania, co z utrwalonych przekonań i nawyków.

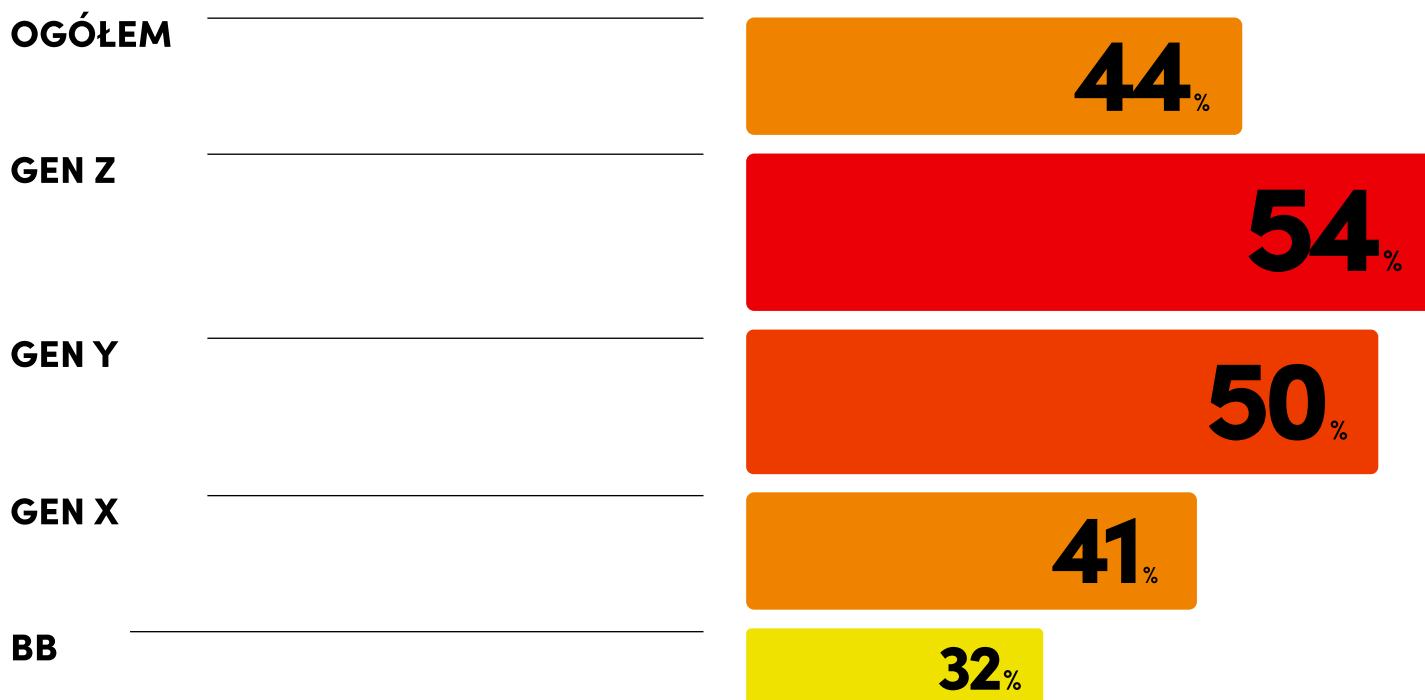
Dodatkową przeszkodą jest postrzegana złożoność rozwiązań. Użytkownicy często uznają dodatkowe zabezpieczenia za skomplikowane, czasochłonne, niewygodne lub obarczone ryzykiem (np. grożące przypadkowym zablokowaniem konta).

W tym kontekście kluczowe znaczenie ma zarówno upraszczanie korzystania z tych rozwiązań, aby były jak najbardziej przyjazne dla użytkowników, jak i działania edukacyjne, które pomagają lepiej zrozumieć sposób działania tych narzędzi i w efekcie zbudują do nich zaufanie.



DOŚWIADCZENIA CYBERATAKÓW CZĘSTSZE WŚRÓD MŁODYCH

DOŚWIADCZENIE OSZUSTWA LUB CYBERATAKU (OSOBIŚCIE LUB WŚRÓD BLISKICH)



Ponad 40% Polaków deklaruje, że oni sami lub osoby z ich otoczenia były celem cyberprzestępców, najczęściej w formie prób wyłudzenia danych lub środków finansowych.

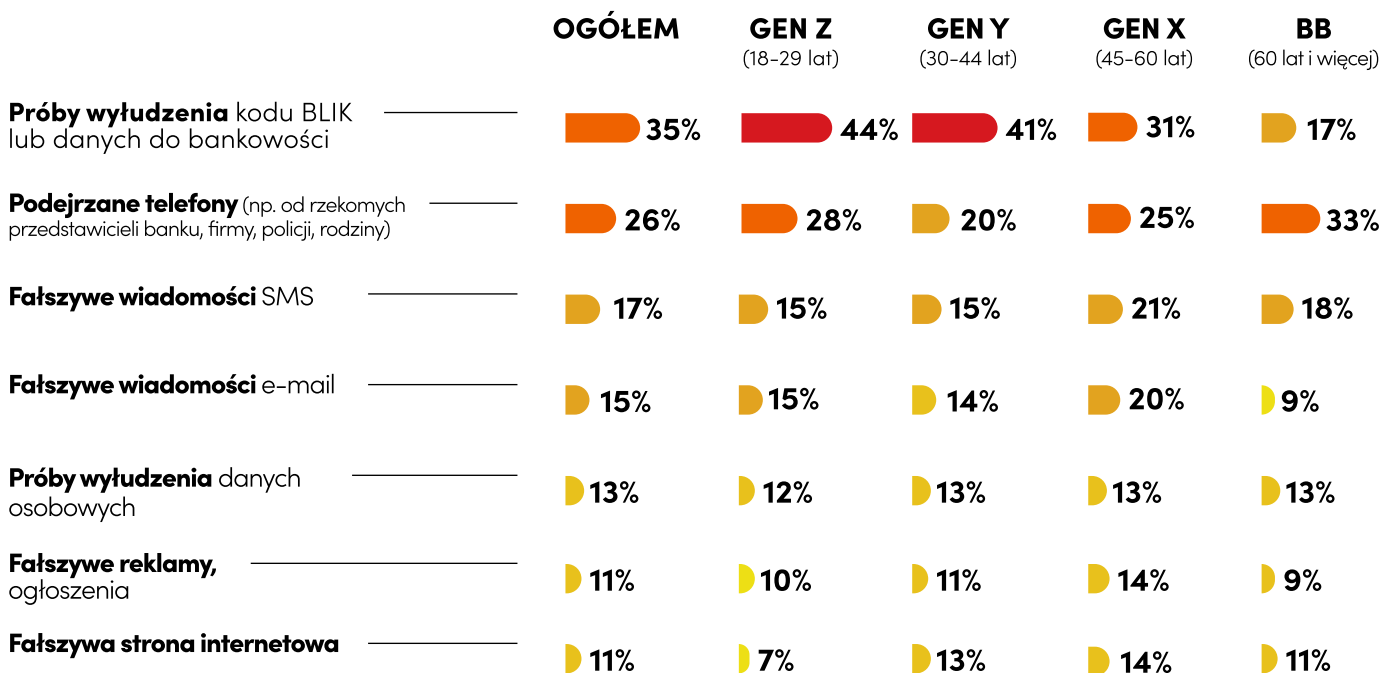
W większości przypadków zgłaszane formy oszustw, czyli wyłudzenia z wykorzystaniem

kodu BLIK, podejrzane telefony i fałszywe SMS-y z linkiem, dobrze oddają charakter współczesnych ataków, w których przestępcy wykorzystują zarówno presję czasu, jak i zaufanie do innych ludzi.

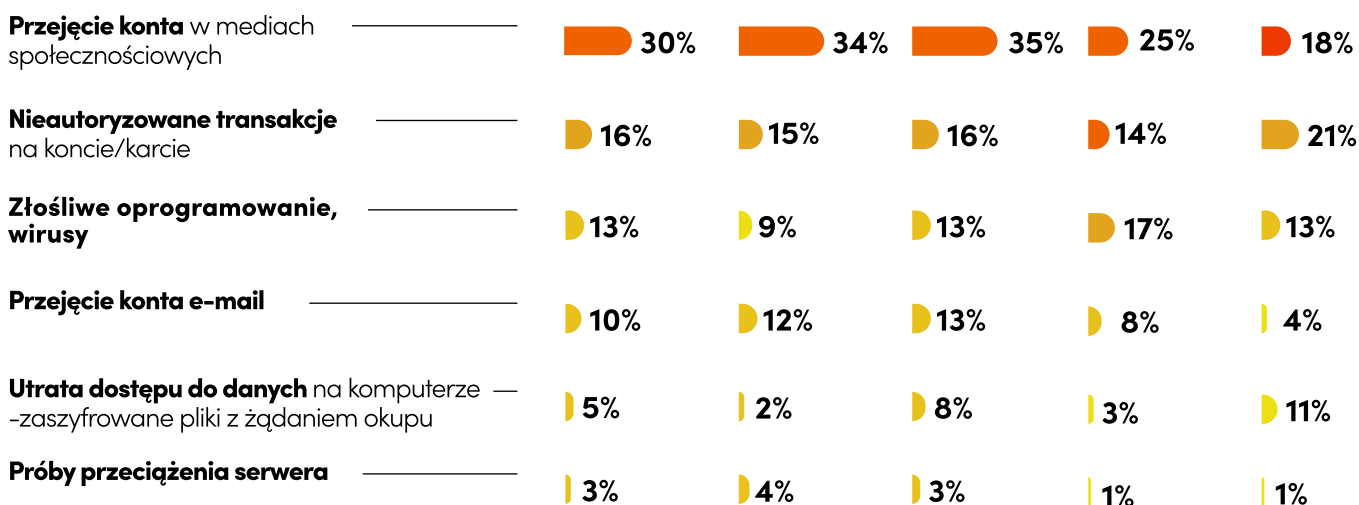
MANIPULACJA NAJCZĘSTSZĄ FORMĄ ATAKU

RODZAJ DOŚWIADCZONEGO OSZUSTWA LUB CYBERATAKU

SOCJOTECHNIKA I WYŁUDZENIA



ATAKI TECHNICZNE, SYSTEMOWE I PRZEJĘCIA



Baza: osoby, które doświadczyły cyberataku lub oszustwa (osobiście lub wśród bliskich)

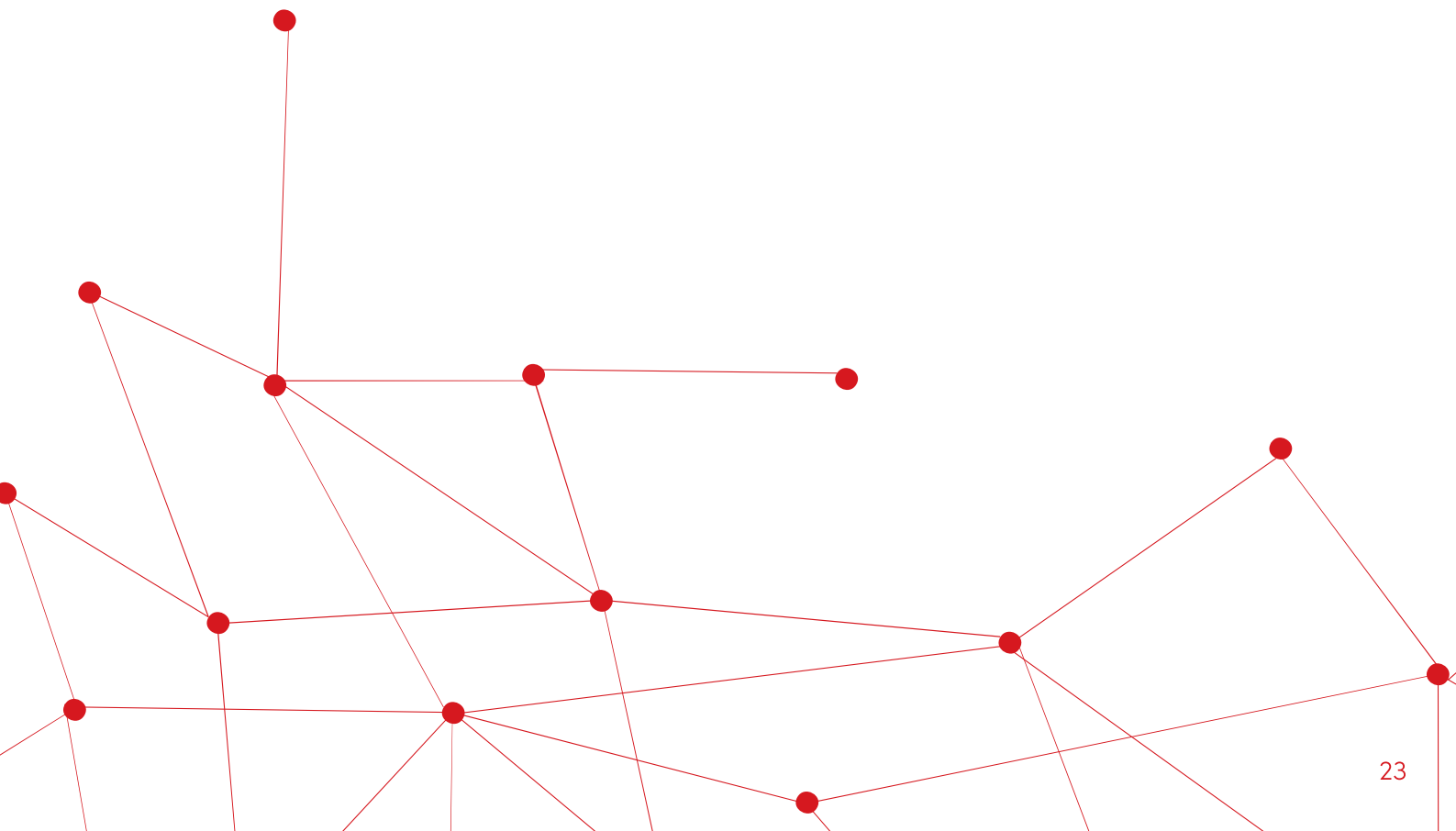
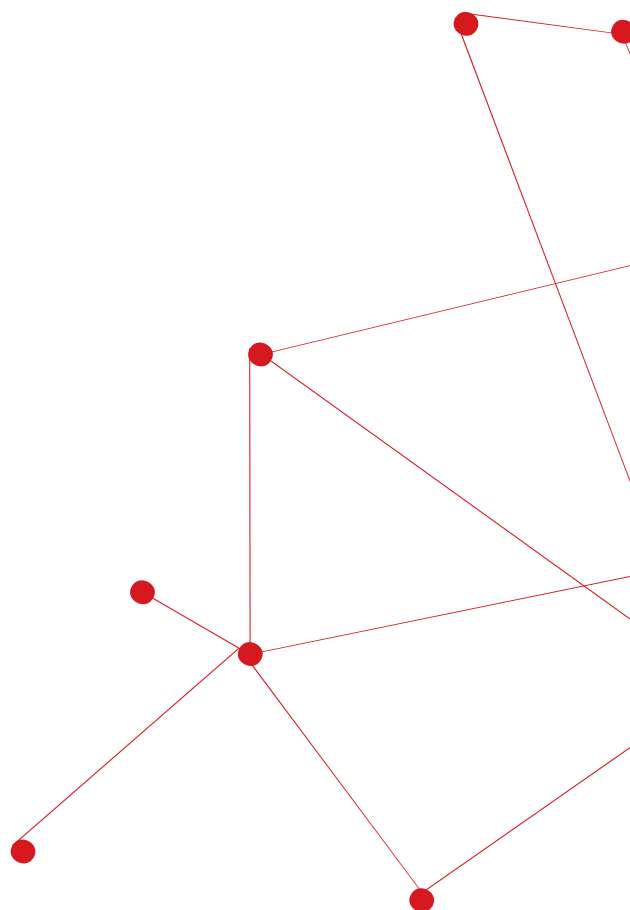
niskie  wysokie

OCHRONA ZACZYNA SIĘ OD CZŁOWIEKA

Wszystkie typy incydentów łączy wspólny mianownik: jest to atak na człowieka, a nie na technologię. Przestępcy wykorzystują emocje i nawyki użytkowników, co sprawia, że nawet osoby świadome zagrożeń mogą paść ofiarą manipulacji.

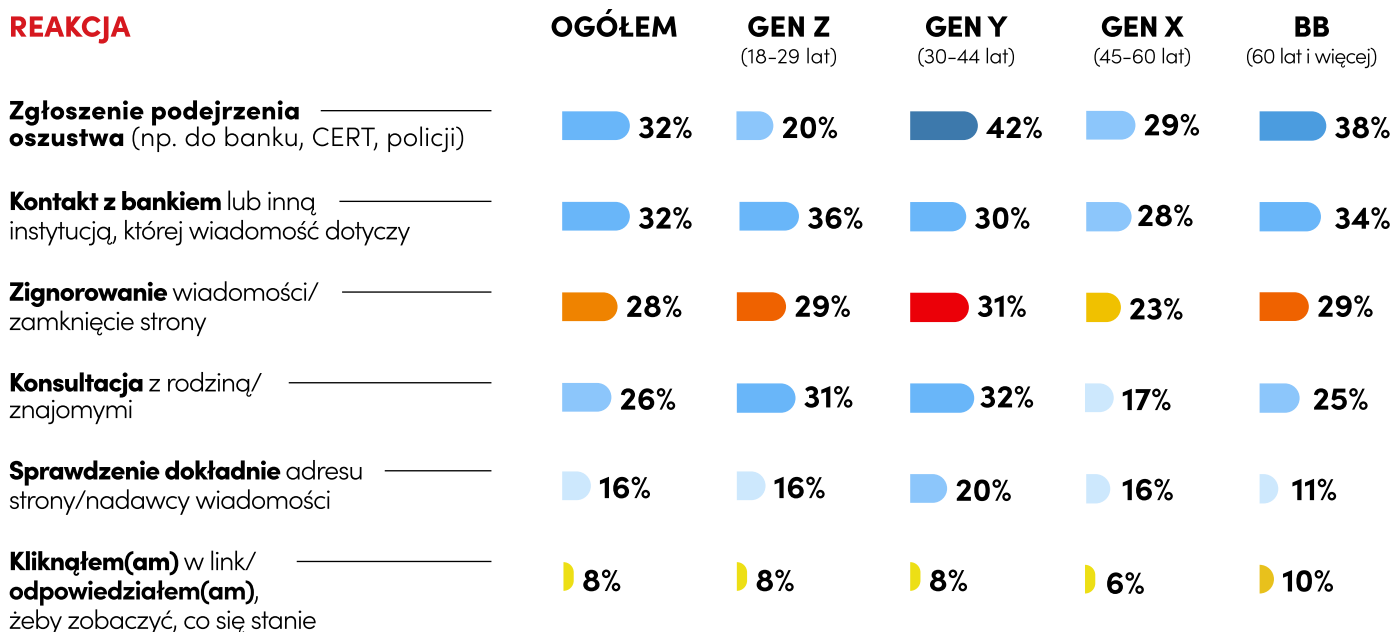
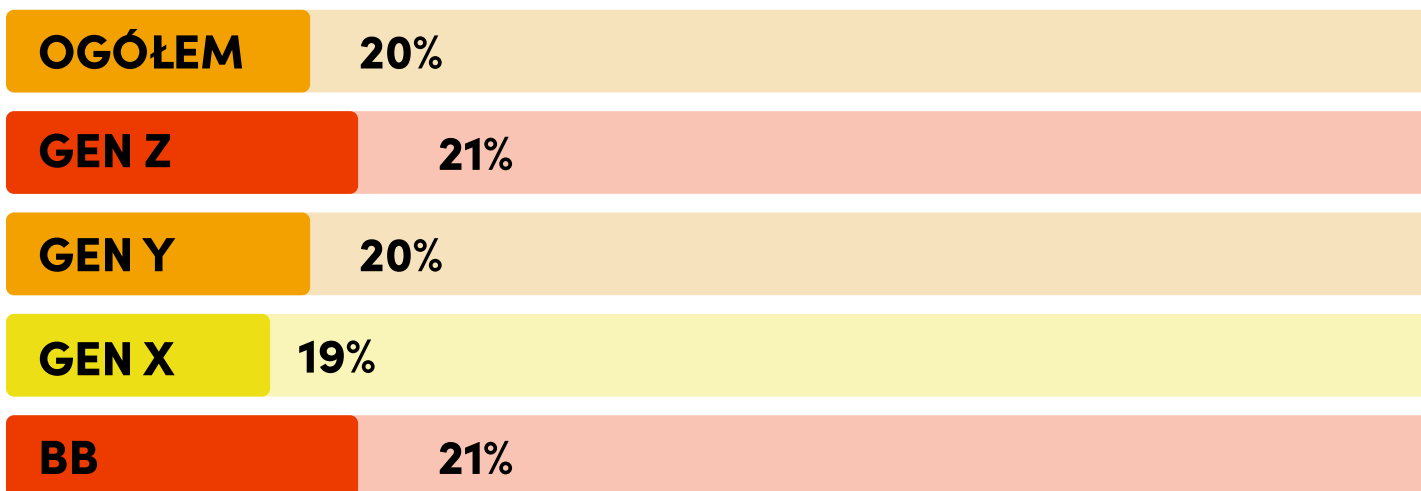
W konsekwencji, znaczenie zyskują działania edukacyjne i budowanie odporności na zagrożenia w sieci. To obejmuje stosowanie zarówno podstawowych zasad higieny cyfrowej, jak i umiejętność rozpoznawania socjotechnik.

Rosnąca skala tych zagrożeń oznacza również konieczność dalszego wzmacniania mechanizmów uwierzytelniania, ograniczania uprawnień aplikacji oraz rozwijania narzędzi do automatycznego wykrywania prób przejęcia tożsamości cyfrowej (np. ochrona behawioralna). Tylko połączenie technologii, procedur i świadomości użytkowników może realnie ograniczyć skuteczność tego typu oszustw.



CO PIĄTY POLAK DOŚWIADCZYŁ PRÓBY OSZUSTWA

OSOBISTE DOŚWIADCZENIE OSZUSTWA LUB CYBERATAKU



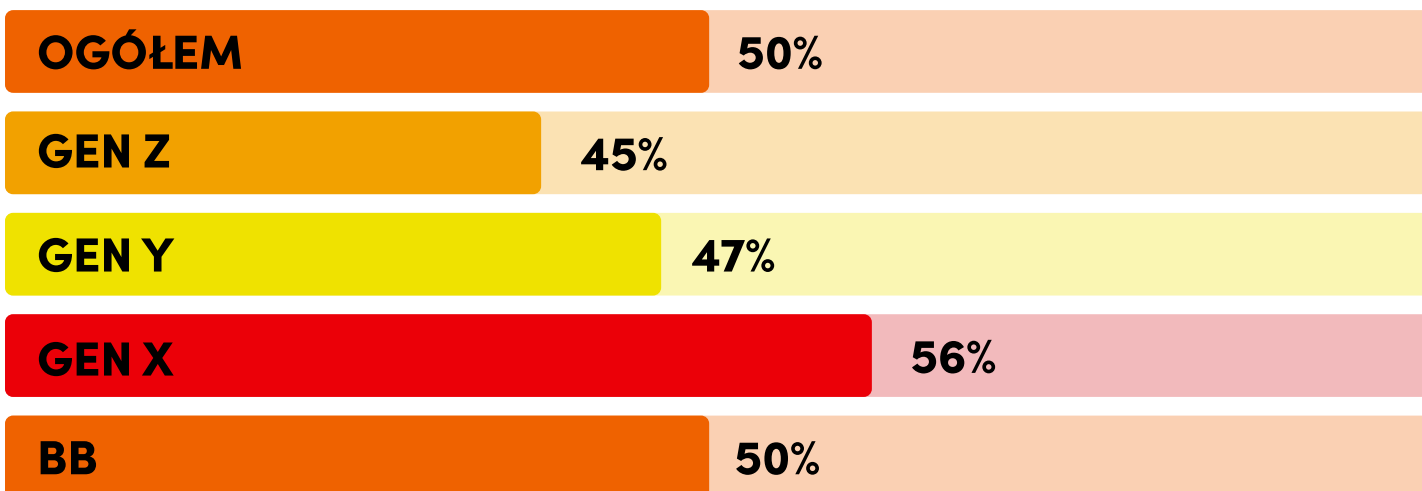
Baza: osoby, które osobiście doświadczyły cyberataku lub oszustwa

Osoby, które padły ofiarą cyberataku, najczęściej podjęły aktywne działania, takie jak zgłoszenie incydentu czy kontakt z odpowiednią instytucją. Dotyczy to jednak jedynie około jednej trzeciej (32%). Zbliżony odsetek respondentów deklaruje, że zignorował zagrożenie (28%). Uwagę zwraca niski poziom zgłaszania incydentów u najmłodszego pokolenia, jest to zaledwie

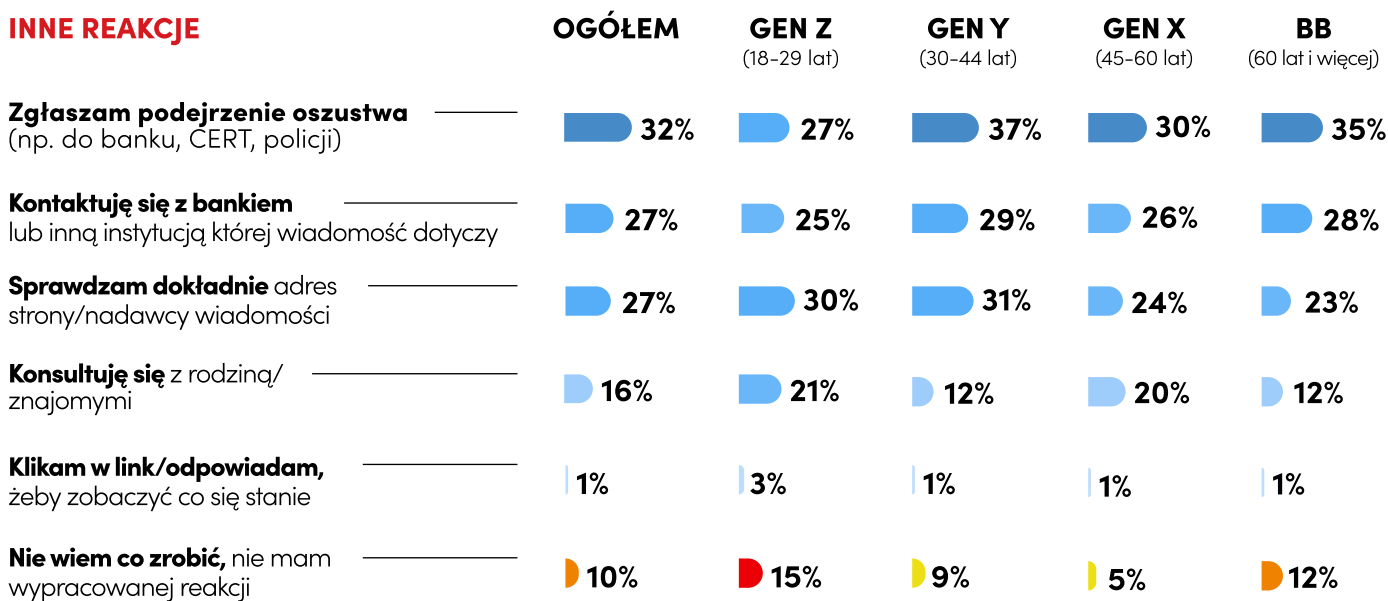
20% przypadków. Co czwarty respondent (26%) w sytuacji ryzyka szuka wsparcia przede wszystkim wśród rodziny lub znajomych, co może pełnić ważną funkcję ochronną. Rozmowa z bliskimi zwiększa szanse na rozpoznanie cyberataku i ograniczenie potencjalnych strat, pod warunkiem, że oni sami są świadomi zagrożeń.

IGNOROWANIE NAJCZĘSTSZĄ REAKCJĄ NA POTENCJALNY CYBERATAK

ZIGNOROWANIE WIADOMOŚCI LUB ZAMKNIĘCIE STRONY



INNE REAKCJE



Baza: osoby, które nie doświadczyły oszustwa ani cyberataku

Wśród osób, które nie doświadczyły cyberataku, aż połowa deklaruje, że gdyby do niego doszło, nie podjęłaby żadnych działań i zignorowałaby taką wiadomość. Taka bierna postawa sprzyja dalszemu rozprzestrzenianiu się ataków i wydłuża czas działania przestępców, którzy mogą wykorzystywać te same metody wobec kolejnych użytkowników. Jednocześnie około jedna trzecia badanych deklaruje gotowość zgłoszenia incydentu lub kontaktu z bankiem,

jednak poziom ten pozostaje relatywnie niski i zbliżony do obserwowanego wśród osób, które faktycznie doświadczyły cyberataku. Warto zauważyć, że najbardziej scyfryzowane pokolenie Z, częściej niż inne generacje, nie wiedziałoby jak zareagować w obliczu zagrożenia (15%). To przeczy powszechnemu przekonaniu, że duże obycie w internecie przekłada się na znajomość właściwych reakcji w niebezpiecznych sytuacjach.



Najczęstszą wskazywaną reakcją na hipotetyczny cyberatak jest jego zignorowanie.

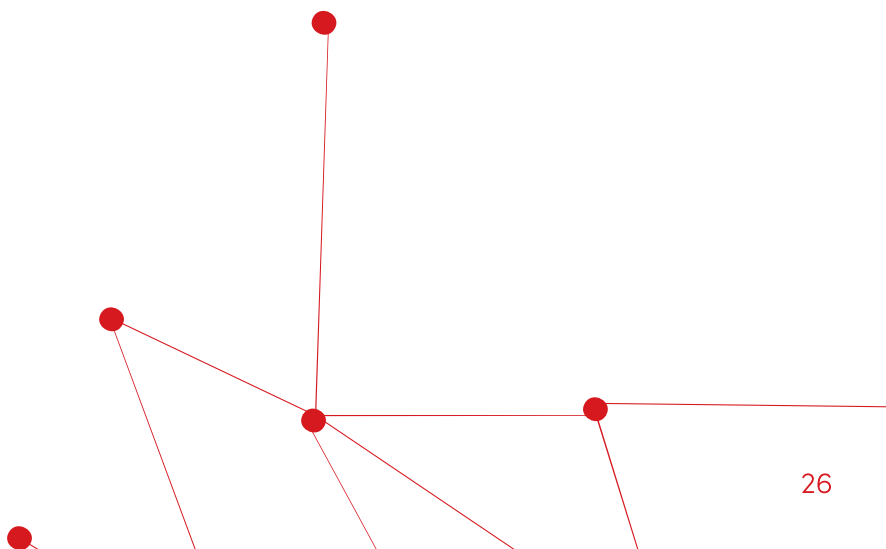
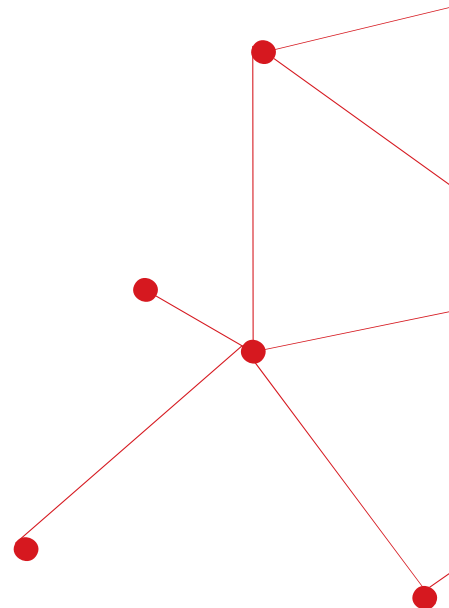
Często słuszną reakcją jest zupełne zignorowanie samej podejrzanej wiadomości czy zamknięcie podejrzanej witryny internetowej. Warto jednak przypomnieć, że istnieje specjalna strona: incydent.cert.pl gdzie można zgłaszać próby cyberataków (np. podejzranego SMS-a). Dzięki temu pomagamy instytucji CERT Polska w jeszcze szybszym reagowaniu na zagrożenia, dzięki czemu chronieni są również inni użytkownicy Internetu.

Inna sytuacja – jeśli otrzymamy wiadomość na komunikatorze od naszego znajomego, a wiadomość wygląda jak wysłana przez cyberprzestępców (np. w wyniku przejęcia konta), to oczywiście warto poinformować o tym znajomego.

Dobłą reakcją w momencie, gdy ktoś rzekomo dzwoni z banku czy Policji i ostrzega np. o cyberataku czy innym problemie bezpieczeństwa, jest rozłączenie się. Następnie warto samodzielnie wybrać numer telefonu danej instytucji i potwierdzić, czy mamy do czynienia z zagrożeniem. W ten sposób niejako przy okazji przekazujemy informację o próbach cyberataku odpowiednim jednostkom, które będą w stanie ochronić osoby posiadające mniejszą od nas świadomość cyberzagrożeń.

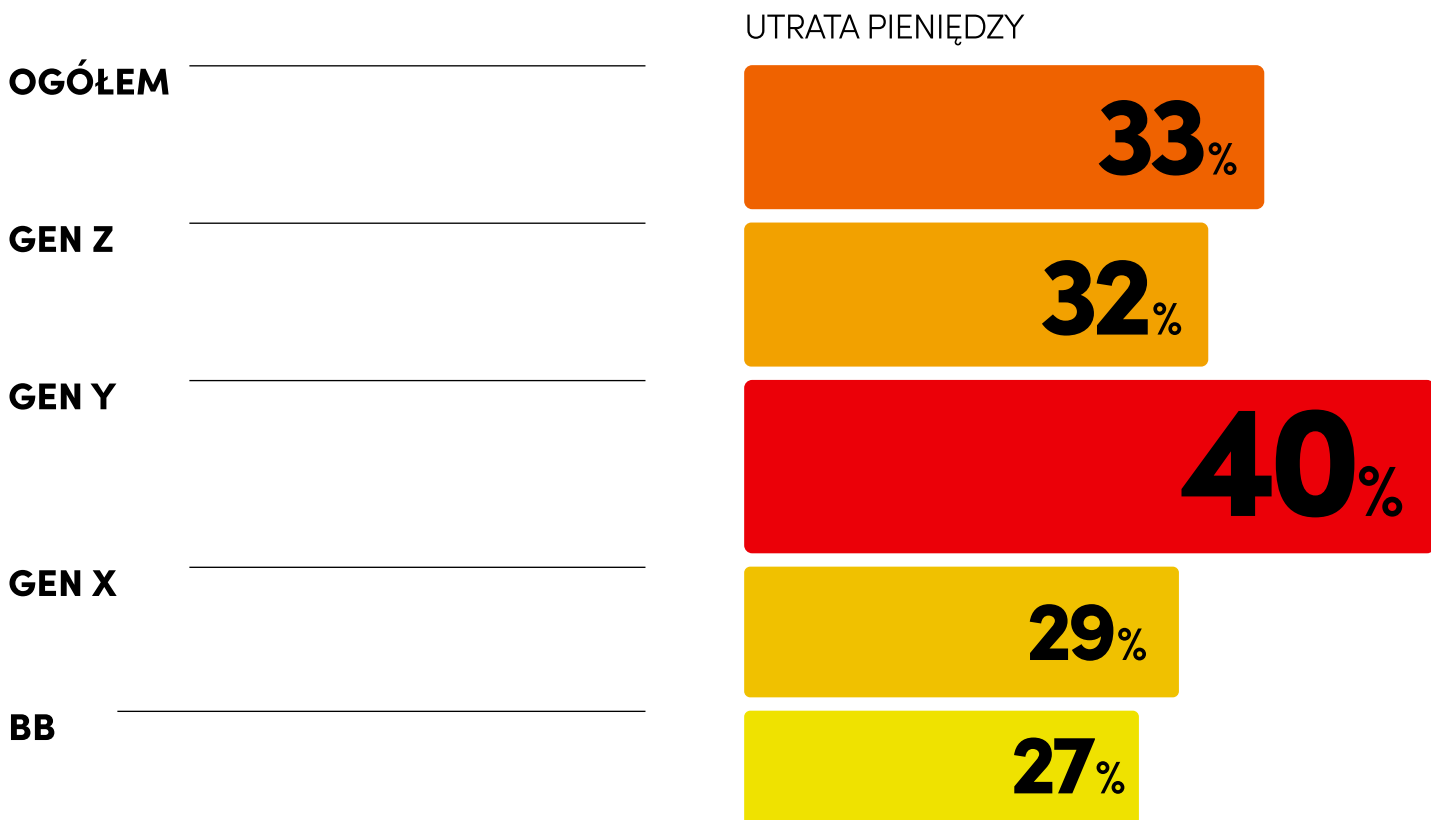


Michał Sajdak,
twórca portalu sekurak.pl,
założyciel Securitum

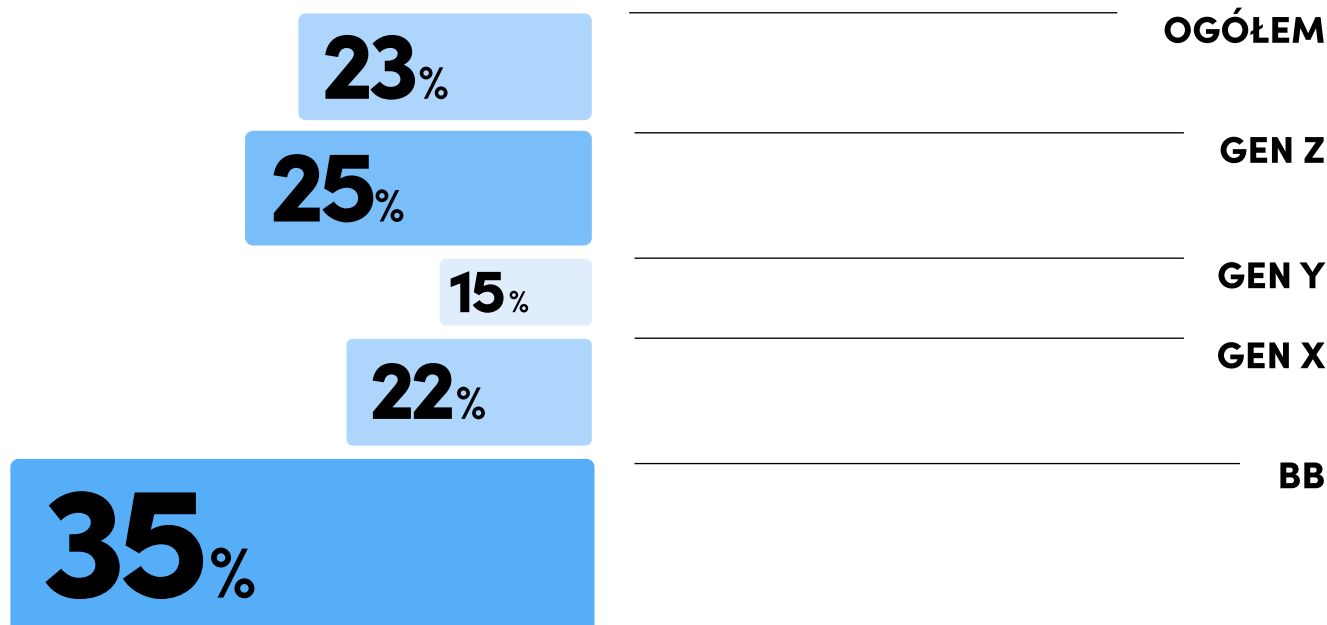


CYBEROSZUSTWA UDERZAJĄ PRZED W SZYSTKIM W FINANSE

NAJCZĘSTSZE SKUTKI CYBERATAKÓW I OSZUSTW INTERNETOWYCH



BRAK JAKICHKOLWIEK KONSEKWENCJI



Baza: osoby, które doświadczyły oszustwa lub cyberataku (osobiście lub wśród bliskich)

CYBERATAKI DOTYKAJĄ TAKŻE WIZERUNKU

INNE SKUTKI CYBERATAKÓW I OSZUSTW INTERNETOWYCH

	OGÓŁEM	GEN Z (18-29 lat)	GEN Y (30-44 lat)	GEN X (45-60 lat)	BB (60 lat i więcej)
Przejęcie konta/tożsamości w mediach społecznościowych	17%	21%	19%	14%	9%
Wykorzystanie danych do podszywania się, by oszukać znajomych	13%	17%	16%	7%	6%
Zablokowanie konta bankowego/aplikacji bankowej	9%	8%	7%	12%	8%
Zainfekowanie urządzeń wirusem	8%	8%	7%	12%	4%
Przejęcie kontroli nad urządzeniami	6%	4%	10%	4%	6%
Utrata danych	6%	7%	7%	4%	5%
Przejęcie kontroli nad skrzynką e-mail	5%	6%	4%	6%	5%
Szantaż	5%	5%	4%	4%	5%
Brak dostawy zakupionego produktu on-line	5%	4%	4%	4%	6%
Wyludzenie kredytu/zaciągnięcie zobowiązań na moje dane	4%	6%	3%	5%	3%
Wgląd w poufne dokumenty	3%	5%	3%	3%	1%
Założenie firmy na skradzione dane	1%	2%	2%	0%	0%

Baza: osoby, które doświadczyły oszustwa lub cyberataku (osobiście lub wśród bliskich)

niskie  wysokie

WYRÓŻNIKI POKOLEŃ

Z Młodsze generacje relatywnie częściej niż inne pokolenia doświadczają przejęcia kont w social mediach.

BB Starsze pokolenia, zwłaszcza Baby Boomersi, częściej deklarują brak odczuwalnych konsekwencji ataku.

Najczęstszym skutkiem cyberoszustw jest utrata pieniędzy (33%), która częściej występuje wśród generacji Y (40%). Kolejne najpopularniejsze skutki dotyczą przejęcia tożsamości, kont (17%) oraz wykorzystania danych osobowych (13%). Wskazuje to, że cyberoszustwa coraz częściej

mają także wymiar wizerunkowy i długofalowy, wykraczający poza same straty finansowe. Z drugiej strony niemal co czwarta osoba (23%) deklaruje brak negatywnych skutków. Pozwala to sugerować, że część incydentów kończy się bez realnych strat lub nie jest w pełni rozpoznawana przez użytkowników.



Nie bez powodu ten raport rozpoczynamy od analizy zachowań różnych pokoleń użytkowników sieci. To właśnie sposób, w jaki Polacy funkcjonują online, w największym stopniu kształtuje ich poczucie bezpieczeństwa, postrzeganie zagrożeń oraz realne podejście do ochrony swoich danych. Szczególnie interesujący obraz wyłania się w przypadku pokolenia Z – najbardziej cyfrowo zaawansowanej grupy. Choć „Zetki” intensywnie korzystają z internetu, rzadziej niż inni odczuwają zagrożenia i rzadziej zakładają, że mogłyby paść ofiarą cyberataku. Można przypuszczać, że wynika to z dużej pewności siebie i poczucia swobody w środowisku cyfrowym, które w ich odczuciu nie skrywa już wielu tajemnic.

Co istotne, to przekonanie nie bierze się znikąd. Pokolenie Z faktycznie częściej niż inni korzysta z zaawansowanych rozwiązań bezpieczeństwa, takich jak uwierzytelnianie dwuskładnikowe czy biometria. Jednak i tu pojawia się kluczowy paradoks, większa technologiczna świadomość nie zawsze idzie w parze z ostrożnością. To właśnie w tej grupie najczęściej obserwujemy ryzykowne zachowania: klikanie w niezweryfikowane linki, logowanie bez sprawdzenia wiarygodności strony czy nieostrożne udostępnianie danych.

Najwyższy poziom czujności pokolenie Z wykazuje w obszarze mediów społecznościowych. Obawy dotyczące przejęcia kont są w tej grupie wyraźnie silniejsze, co znajduje odzwierciedlenie w doświadczeniach. Młodzi użytkownicy częściej mają styczność z cyberatakami i relatywnie częściej doświadczają kradzieży tożsamości właśnie w social mediach. Podobny mechanizm widoczny jest w pokoleniu Y.

W ich przypadku większe obawy, zwłaszcza przed utratą środków finansowych, mogą wynikać z częstszego kontaktu z konsekwencjami tego typu incydentów.

Dane jednoznacznie pokazują, że sama znajomość narzędzi i korzystanie z nowoczesnych zabezpieczeń nie są wystarczające. Co więcej, mogą tworzyć złudne poczucie kontroli. W świecie cyfrowym to nie tylko technologia, ale przede wszystkim codzienne nawyki decydują o bezpieczeństwie. A wysoka aktywność online, połączona z brakiem ostrożności, niezmiennie zwiększa ekspozycję na zagrożenia i ryzyko ataku.



Patryk Korus,
Dyrektor Biura Aktywizacji Kanałów
i Procesów Cyfrowych

ZAKOŃCZENIE

Pierwsza część naszego raportu pokazuje obraz cyfrowej codzienności Polaków: jesteśmy online po kilka godzin dziennie, korzystamy z bankowości internetowej, robimy zakupy, załatwiamy sprawy na smartfonie. Internet stał się naszym naturalnym środowiskiem: wygodnym, szybkim i wszechobecnym.

Ale wraz z tą wygodą rośnie też odpowiedzialność za własne bezpieczeństwo. Najważniejsza historia, jaką opowiadają dane przedstawione w raporcie, to historia luki pomiędzy wiedzą i działaniem. Większość z nas zna podstawowe zagrożenia i potrafi je nazwać. Wiemy, jakie zagrożenia na nas czekają oraz jak możemy się przed nimi chronić, a jednak w praktyce działamy inaczej: klikamy w link „na szybko”, logujemy się do serwisów bez sprawdzenia adresu, odkładamy włączenie dodatkowych zabezpieczeń.

Paradoks polega na tym, że jednocześnie korzystamy z internetu coraz intensywniej, coraz lepiej rozumiemy zagrożenia, ale tylko częściowo przekładamy tę wiedzę na konkretne i codzienne decyzje.

Niestety cyberprzestępcy wykorzystują właśnie ten moment chwili nieuwagi, rutyny, działania pod wpływem emocji. Z danych wyłania się jeszcze jeden ważny wniosek: w cyberbezpieczeństwie najstabszym i równocześnie najmocniejszym ogniwem jest człowiek. To od naszych codziennych wyborów zależy, czy zabezpieczenia przed cyberoszustwami i cyberatakami zadziałają.

Dlatego przyszłość bezpieczeństwa nie polega wyłącznie na tworzeniu coraz bardziej zaawansowanych narzędzi. Kluczowe jest coś znacznie bliższego codzienności:

- proste rozwiązania, które łatwo włączyć,
- jasne komunikaty, które podpowiadają co zrobić,
- edukacja, która będzie systematycznie przypominać jak się chronić w cyberprzestrzeni,
- nawyki, które działają nawet wtedy, gdy jesteśmy zmęczeni, rozproszeni albo w pośpiechu.

Bo bezpieczeństwo w sieci nie dzieje się od czasu do czasu, ale przy każdym naszym kliknięciu.

W drugiej części raportu zaprezentujemy jak podchodzimy do bezpieczeństwa w obszarze bankowości mobilnej, czyli tam, gdzie bezpieczeństwo klienta spotyka się z konkretnymi rozwiązaniami, funkcjami i wsparciem na co dzień. Omówimy, jak Polacy oceniają poziom ochrony swoich środków finansowych w bankach, z jakich rozwiązań zabezpieczających korzystają podczas używania bankowości internetowej i aplikacji mobilnych oraz jakie mają oczekiwania względem inicjatyw edukacyjnych banków dotyczących bezpieczeństwa w świecie cyfrowym.

