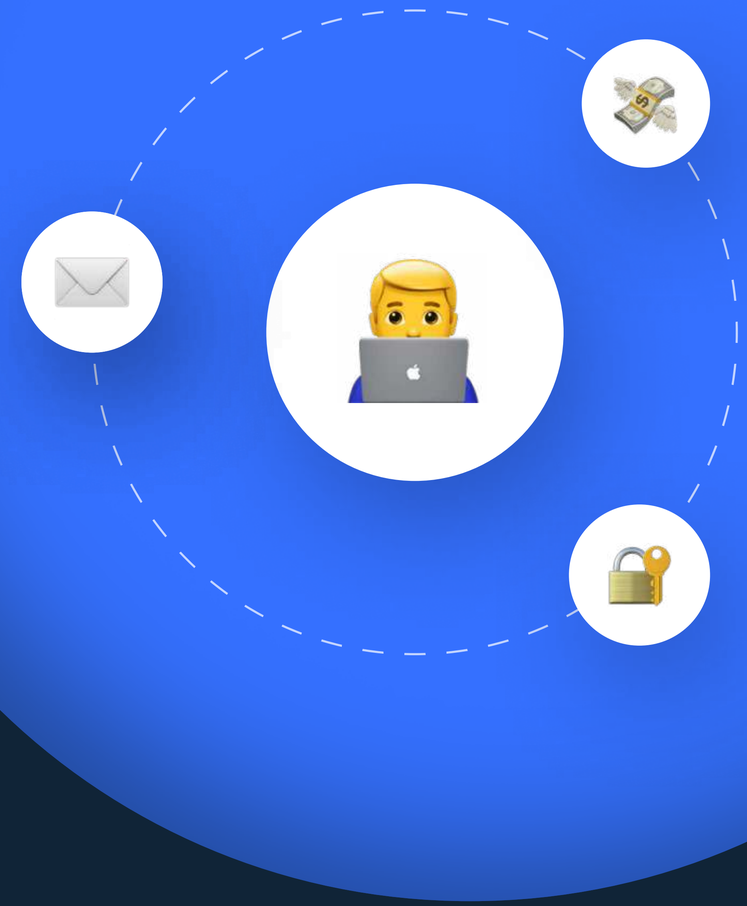
SMSAPI

Bezpieczeństwo cyfrowe Polaków 🔓

Oszustwa internetowe i zagrożenia komunikacji mobilnej



> Jak bronić się przed **oszustwami internetowymi**?

Raport SMSAPI 2024

Spis treści

Wstęp

Wojciech Kaczmarek jest związany z marką SMSAPI od ponad 15 lat. Pełni funkcję **Dyrektora Zarządzającego w LINK Mobility Poland** – części międzynarodowej grupy zrzeszającej czołowych dostawców komunikacji SMS dla biznesu.

Wojciech Kaczmarek
Dyrektor zarządzający
LINK Mobility Poland

Marka SMSAPI od ponad 16 lat dostarcza profesjonalne rozwiązania w zakresie masowej wysyłki wiadomości SMS dla firm i instytucji publicznych w Polsce i na całym świecie. Dzisiaj stoimy przed **jednym z najważniejszych wyzwań współczesności** – zagrożeniami płynącymi z cyberprzestrzeni, które bezpośrednio wpływają na nasze życie prywatne i zawodowe. Ochrona danych, tożsamości oraz bezpieczeństwo komunikacji elektronicznej to realne problemy dla biznesu, sektora publicznego, a także wszystkich Polaków.

Powszechne kanały komunikacji, takie jak **SMS czy e-mail,** cieszą się ogromną popularnością i zaufaniem wśród odbiorców na całym świecie. Niestety ich popularność czyni je **atrakcyjnym celem dla oszustów**.

Żerując na niewiedzy, rozproszonej uwadze i często pośpiechu, znajdują w nich skuteczne narzędzie dotarcia do podatnych lub słabiej poinformowanych osób.

Wyzwanie jest adresowane przez wszystkich uczestników ekosystemu gospodarczego. Ustawa z 28 lipca 2023 roku o zwalczaniu nadużyć w komunikacji elektronicznej to ważny krok w kierunku zwiększenia bezpieczeństwa cyfrowego Polaków. Wprowadzenie jasnych regulacji i kar dla osób, które wykorzystują technologie do oszustwa to sygnał dla rynku, że **bezpieczeństwo użytkowników internetu jest na pierwszym planie.**

Wstęp cd.

Jako firma świadcząca usługi SMS dla firm i instytucji publicznych, rozumiemy wagę bezpieczeństwa komunikacji elektronicznej. Widząc rosnące zagrożenia, postanowiliśmy przygotować raport, który odpowiada na **kluczowe pytania dotyczące oszustw internetowych w Polsce**, takie jak identyfikacja narażonych grup wiekowych czy metody rozpoznawania ataków typu phishing.

Przeprowadzone przez nas badanie wskazuje na niepokojący wzrost przypadków phishingu SMS i e-mail. **54% ankietowanych przyznaje, że otrzymało wiadomość zawierającą podejrzane treści.** Perfidne metody ataku mają między innymi na celu wyłudzenie od odbiorców cennych informacji poufnych, często prowadząc do poważnych konsekwencji finansowych. Zapraszam do zapoznania się z wynikami badania, poradami oraz komentarzami ekspertów.

Pamiętajmy, że bezpieczeństwo cyfrowe Polaków to nie tylko kwestia technologii. To także **kwestia kultury cyfrowej, edukacji i świadomości.**

Wojciech Kaczmarek – LINK Mobility Poland

Skrót z raportu

Trzy rady:

#1 **Czytaj uważnie** otrzymywane komunikaty

#2 **Pomyśl** zanim podasz dane

#3 **Rozmawiaj** i dziel się doświadczeniem

Najważniejsze wnioski:

- **17,8%** padło ofiarą oszusta internetowego
- **53,7%** otrzymało podejrzane treści
- **61,9%** sądzi, że potrafi rozpoznawać fałszywe komunikaty
- **29,9%** poprawnie wskazało fałszywe komunikaty
- **51,6%** sprawdza adresy i nadawców
- **74%** uważa kod SMS za bezpieczną metodę logowania
- **Połowa** woli załatwiać ważne sprawy osobiście
- **45,9%** ostrzega najbliższych o niebezpieczeństwach
- **53,8%** dowiaduje się o niebezpieczeństwach od najbliższych

Raport **Bezpieczeństwo cyfrowe Polaków** został opracowany przez SMSAPI. Dane pochodzą z badania przeprowadzonego metodą CAWI za pomocą portalu SurvGo. Próba badawcza to 1000 mieszkańców Polski powyżej 18 roku.

Jaka jest **skala problemu?**

7. Czy w ciągu ostatnich sześciu miesięcy padłaś/eś ofiarą oszustwa internetowego?

8. Wskaż grupę wiekową, która według Ciebie jest najbardziej narażona na oszustwa internetowe.

9. Czy w ciągu ostatnich sześciu miesięcy otrzymałaś/eś wiadomości zawierającą podejrzane treści?

10. Jakim kanałem otrzymałaś/eś podejrzane treści?

11. Komentarz: **Leszek Tasiemski**

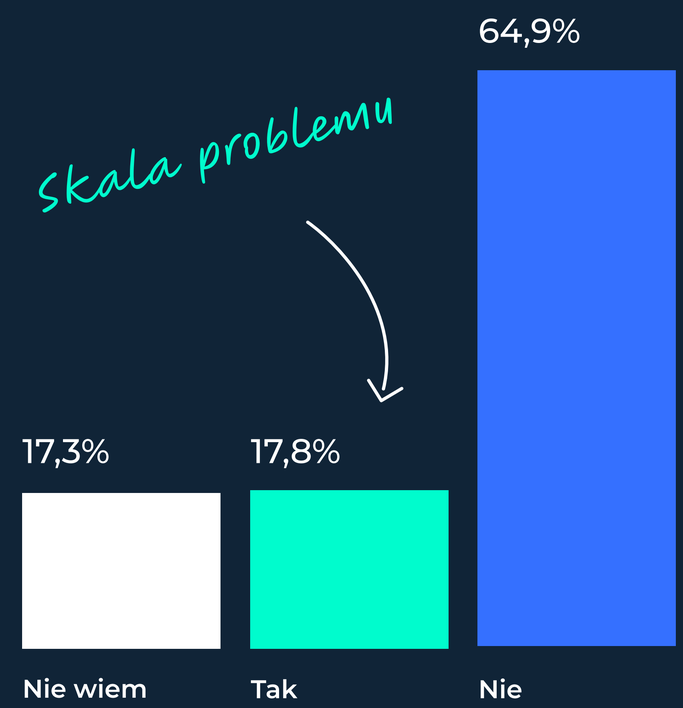
oszustwo internetowe

Wszelkie próby nadużyć w sieci, których celem jest między innymi wyłudzenie pieniędzy, kradzież danych, tożsamości lub uzyskanie nieuprawnionego dostępu do systemów czy informacji.

Skala oszustw internetowych

Z badania wynika, że niemal co piąty ankietowany (**17,8% odpowiedzi**) padł ofiarą oszustwa internetowego.

Czy w ciągu ostatnich sześciu miesięcy **padłaś/eś ofiarą oszustwa** internetowego?

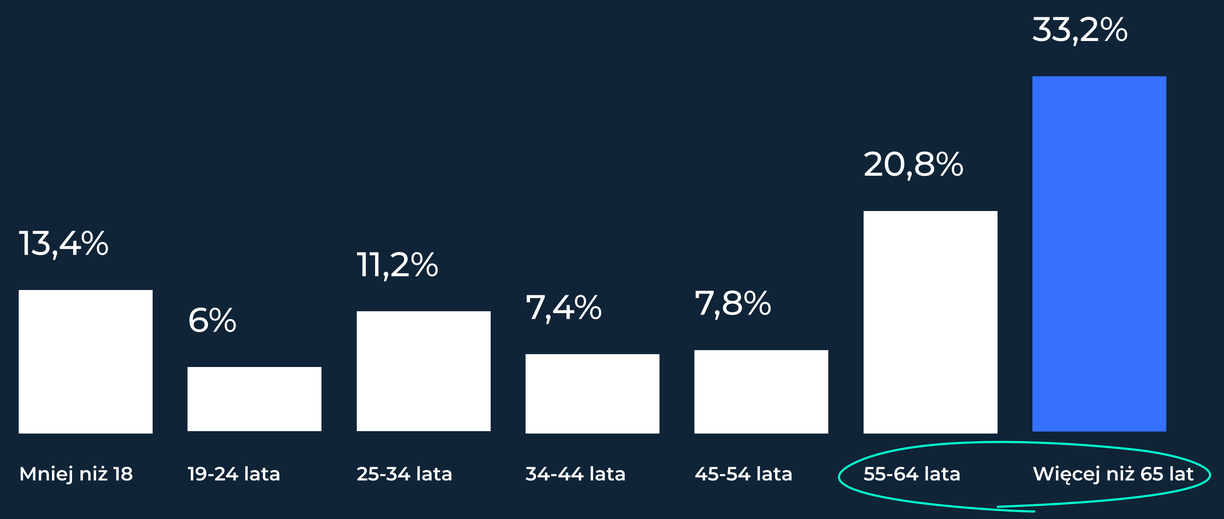


Wiek a **podatność na oszustwa** w sieci

Według większości ankietowanych (**54%**) najbardziej narażoną grupą są osoby po 55 roku życia.

Ankietowani uważają, że zwiększona podatność na oszustwa występuje także wśród osób poniżej 18 roku życia (**13,4%**).

Wskaż **grupę wiekową**, która według Ciebie jest **najbardziej narażona** na oszustwa internetowe.

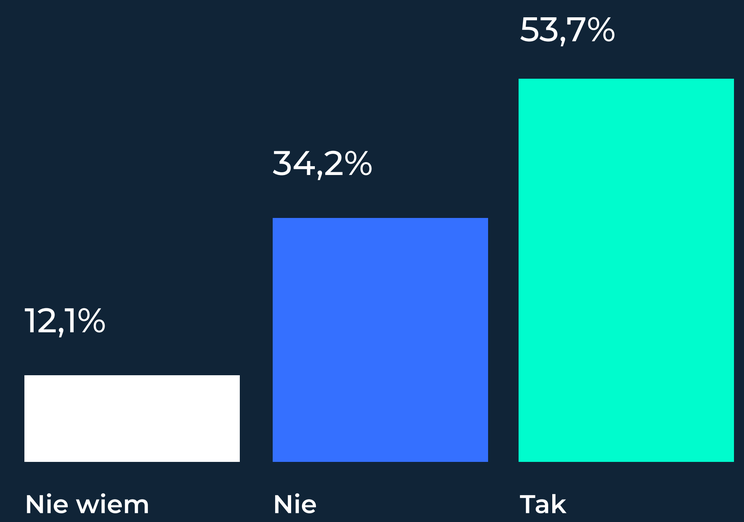


Otrzymywanie **podejrzanych treści**

Co drugi ankietowany (**53,7%**) otrzymał podejrzane treści np. niespodziewane ponaglenie do zapłaty, prośbę o dopłatę za dostawę czy próby wyłudzenia danych lub podszycia się pod urząd, bank, firmę.

Dodatkowe **12,1% ankietowanych nie jest pewne**, czy nie otrzymało wiadomości z próbą oszustwa lub wyłudzenia.

Czy w ciągu **ostatnich sześciu miesięcy** otrzymałaś/eś wiadomość zawierającą **podejrzane treści**?

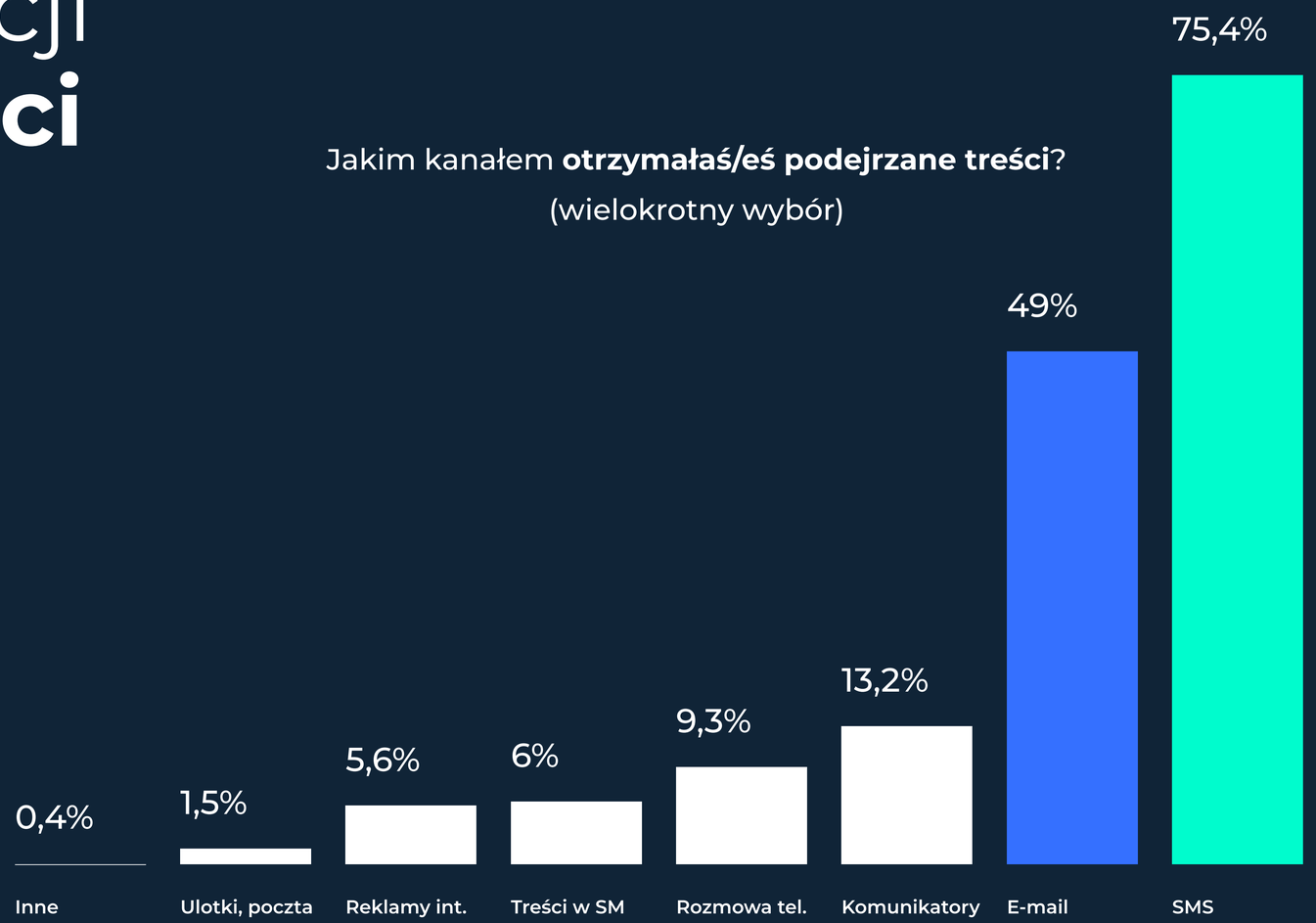


Kanały komunikacji a **podejrzane treści**

Wiadomości e-mail i SMS to najpopularniejsze kanały biznesowej komunikacji mobilnej. Za ich pomocą firmy, urzędy i instytucje publiczne przekazują **ważne informacje oraz prowadzą działania marketingowe**. Oba kanały są także najczęściej wykorzystywane przez oszustów.

Przy okazji warto zwrócić uwagę na komunikatory internetowe oraz rozmowy telefoniczne, które zostały wskazane jako narzędzia oszustw internetowych przez odpowiednio **13,2% i 9,3%** ankietowanych.

Jakim kanałem **otrzymałaś/eś podejrzane treści**?
(wielokrotny wybór)



Komentarz

Leszek Tasiemski jest odpowiedzialny za globalny rozwój technologii w firmie WithSecure. **Posiada 17-letnie doświadczenie w branży cyberbezpieczeństwa** m.in. w przeprowadzaniu testów penetracyjnych oraz analiz powłamaniowych, głównie dla europejskiego sektora finansowego. Entuzjasta zastosowań sztucznej inteligencji w wykrywaniu cyberataków. Absolwent Informatyki, Ekonomii oraz MBA.

Leszek Tasiemski
Vice President of Product Management
WithSecure

Ekspert raportu

Dane potwierdzają, że **internetowa przestępczość stała się codziennością.** Jest wszechobecna, widoczna dla zwykłych użytkowników sieci i dotyczyć może każdego. Niemal **co piąta osoba potwierdza, że padła ofiarą oszustwa.** Co ciekawe, podobny odsetek respondentów nie wie, czy zostało dotkniętych atakiem ze strony cyberprzestępców. Wskazuje to na **niską świadomość społeczeństwa w tym obszarze i potrzebę edukacji.** Trzeba też pamiętać jednak, że czasami trudno jest określić, czy jesteśmy ofiarą.

Jeżeli na przykład zostaną wykradzione nasze dane, może to być zupełnie nie do wychwycenia. Oczywiście tylko do momentu aż informacje te zostaną wykorzystane w fizycznym świecie – na przykład do dokonania transakcji czy przejęcia konta. Istnieją strony internetowe np. Have I Been Pwned, które umożliwiają **sprawdzenie czy nasz adres mailowy był elementem wycieku**.

Interesujące jest, że **jedynie połowa badanych** potwierdza, że zdarzyło się im się **otrzymać podejrzane treści.** Trudno sobie wyobrazić, że aktywny użytkownik sieci nie dostaje w ogóle tego typu wiadomości, np. prób wyłudzenia danych, zachęty do klikania w niebezpieczne linki. Paradoksalnie może to oznaczać, że **dla części badanych tego typu treści są już na tyle powszechne, że stały się częścią szumu informacyjnego**, więc nawet nie zwracają na nie uwagi.

Komentarz cd.

Leszek Tasiemski jest odpowiedzialny za globalny rozwój technologii w firmie WithSecure. **Posiada 17-letnie doświadczenie w branży cyberbezpieczeństwa** m.in. w przeprowadzaniu testów penetracyjnych oraz analiz powłamaniowych, głównie dla europejskiego sektora finansowego. Entuzjasta zastosowań sztucznej inteligencji w wykrywaniu cyberataków. Absolwent Informatyki, Ekonomii oraz MBA.

Leszek Tasiemski
Vice President of Product Management
WithSecure

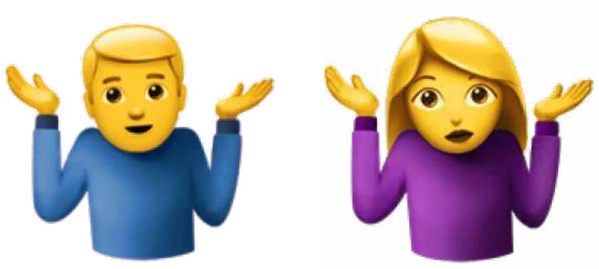
Ekspert raportu

Wiadomości SMS i e-maile to tradycyjnie najpopularniejsze medium ataku. Coraz częściej jednak spotykamy się również z **alternatywnymi kanałami,** np. WhatsApp. Mają one dla przestępców tę zaletę, że są szyfrowane w sposób uniemożliwiający operatorowi monitorowanie przesyłanych treści. Utrudnia to wykrycie i blokowanie ataku.

Ankietowani jako najbardziej narażoną na internetowe oszustwa wskazali osoby starsze. Czynnikiem ryzyka jest tu niska znajomość technologii i związanych z nią zagrożeń. Jednak z drugiej strony taka obiegowa opinia może być mylna. **Osoby starsze podchodzą do internetowych transakcji z niezwykłą ostrożnością, a często nawet z lękiem.** Faktycznie jest to grupa szczególnie często brana na celownik przez **ataki hybrydowe:** z ofiarą kontaktuje się np. przez telefon, ktoś podszywający się pod instytucję lub bliską osobę. Następnie nakłania do wykonania określonej akcji w sieci, która skutkuje np. kradzieżą pieniędzy.

W przypadku cyberbezpieczeństwa najważniejsza jest świadomość. Istotne jest też zachowanie czujności oraz nieograniczanie się tylko do teorii. Wiele firm już przeprowadza **regularne symulacje ataków phishingowych**. Pomagają one wyczulać pracowników na potencjalne zagrożenia. Błędy najczęściej popełniane są w pośpiechu, **gdy ofiara czuje, że nie ma czasu na analizę otrzymanej wiadomości.** Szczególnie skuteczne jest to kiedy otrzymane treści „pasują” do sytuacji. Dlatego w okresie świątecznym mamy wysyp oszustw polegających na podszywaniu się pod firmy kurierskie. Kiedy jest pora rozliczenia PIT – cyberprzestępcy mogą udawać przedstawicieli Urzędu Skarbowego.

Co to jest **phishing?**



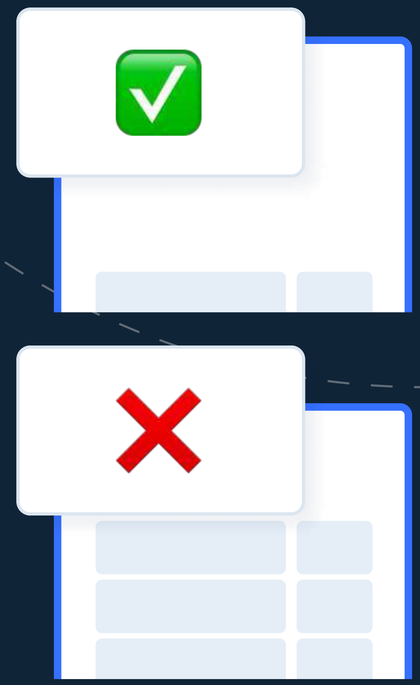
Rozpoznawanie
fałszywych komunikatów

Wedle zebranych odpowiedzi tylko 4,8% miałoby problem z rozpoznaniem fałszywego komunikatu. Co trzeci ankietowany nie jest w stanie jednoznacznie tego stwierdzić. Przeważająca część, bo aż **61,9% sądzi, że potrafi wskazać fałszywe komunikaty**.

Odpowiedzi zostały poddane testowi. **Respondenci mieli wskazać podrobione wiadomości** spośród zaprezentowanych przykładów. Trzy stanowiły próbę oszustwa, a jeden był typowym, autentycznym SMS-em wysłanym przez jedną z polskich firm.

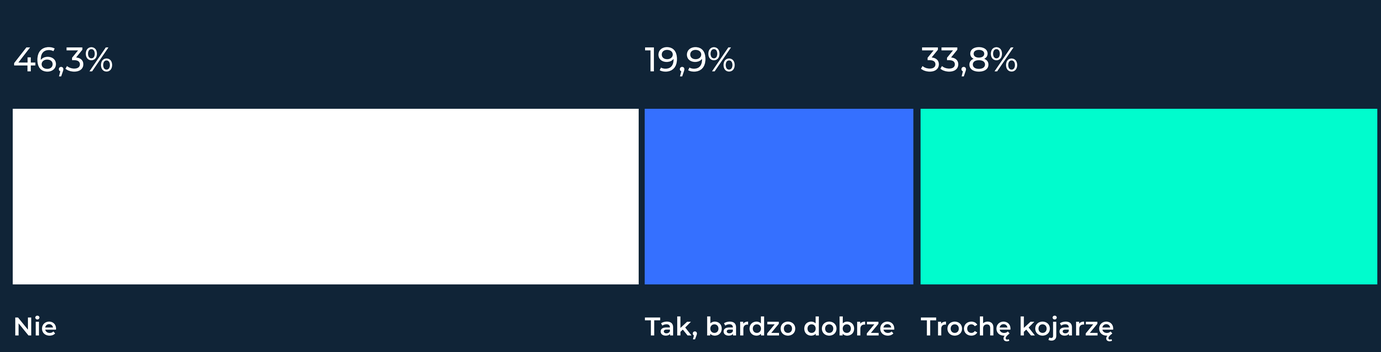
Czy potrafisz **rozpoznać fałszywe** komunikaty?

- **29,89%** wykonało zadanie poprawnie: wskazało tylko trzy fałszywe komunikaty
- **47,33%** wskazały wszystkie wiadomości jako fałszywe
- **53,31%** wskazało prawdziwą wiadomość jako fałszywą



Wiedza na temat **phishingu**

Czy wiesz, **co to jest i na czym** polega phishing?



Definicja **phishingu**

phishing

Forma ataku oparta na fałszywych wiadomościach wysyłanych przez oszusta. Celem jest podszycie się pod znaną firmę, urząd, bank czy instytucję, aby wyłudzić dane, pieniądze lub uzyskać dostęp do systemu.

Wybrane odpowiedzi na pytanie otwarte
Czym dla Pana/i jest *phishing*?

NIE KOJARZĘ WYŁUDZENIE DANYCH ORAZ INFORMACJI PRZEZ INTERNET NIE PAMIETAM PODSTEPNE EMAILE? BEZPIECZEŃSTWO TRUDNO SZYBKO WYTŁUMACZYĆ PODSZYWANIE SIĘ POD CZYJEŚ KONTO NIE WIEM PRÓBA WYŁUDZENIA/OSZUSTWA, SZCZEGÓLNIE DANYCH JEST TO RODZAJ OSZUSTWA INTERNETOWEO. POLEGA GŁÓWNIE NA WYŁUDZENIU DANYCH NP. BANKOWYCH METODA OSZUSTWA W KTÓREJ PRZESTĘPCA PODSZYWA SIĘ POD JAKĄŚ INSTYTUCJE NP. BANK KOLEJNA METODA NA OSZUSTWA WYŁUDZENIEM DANYCH INTERNETOWE PRZESTĘPSTWA PODSZYWANIE SIĘ POD INNĄ OSOBĘ, FIRMĘ, INSTYTUCJĘ COŚ Z TYM ŻE KRADZIEŻY PIENIĘDZY Z BANKU, ZAWIERANIA POŻYCZEK UDAWANIE KONTAKTU OD PRAWDZIWEJ FIRMY TO PRZEMOC PSYCHICZNA ZAGROŻENIE W SIECI TRUDNO POWIEDZIEĆ ŁOWIENIE OFIAR KRADNĄ NASZE DANE PODSZYWANIE SIĘ POD INNĄ OSOBĘ LUB INSTYTUCJĘ W CELU WYŁUDZENIA POUFNYCH DANYCH RODZAJ CYBERATAKU, PODCZAS KTÓREGO CYBERPRZESTĘPCA PRÓBUJE **WYŁUDZIĆ**

OD OFIARY POUFNE INFORMACJE WYŁUDZANIE DANYCH OSOBOWYCH JAK NUMER PESEL SKAN DOWODU DANE BANKOWE ABY JE ODSPRZEDAĆ BĄDŹ UŻYĆ W CELU OSZUSTWA PODSZYWANIEM SIĘ METODA OSZUSTWA, W KTÓREJ PRZESTĘPCA PODSZYWA SIĘ POD INNĄ OSOBĘ LUB INSTYTUCJĘ W CELU WYŁUDZENIA POUFNYCH INFORMACJI PODSZYWANIE SIĘ POD KOGOŚ INNEGO W CELU WYŁUDZENIA RÓŻNYCH DANYCH OSOBISTYCH OSZUSTWO POLEGAJĄCE NA PODAWANIU SIĘ ZA INNĄ OSOBĘ (NIŻ TA, KTÓRĄ JEST SIĘ), ABY WYŁUDZIĆ DANE PODSZYWANIE SIĘ POD KOGOŚ I WYKORZYSTYWANIE INNYCH DZIĘKI TEMU PODSZYWANIE SIĘ POD PODMIOT OSZUST2A INTERNETOWE PODSZYWANIE SIĘ POD INNĄ OSOBĘ W CELU WYŁUDZENIA DANYCH WRAŻLIWYCH KRADZIEŻĄ DANYCH OSOBOWYCH KRADZEŻ TOŻSAMOŚCI KRADZIEŻ DANYCH OSOBOWYCH WYLUDZANIE DANYCH PODSZYWAJAC SIE NP. POD PRACOWNIKA FIRMY POPRZEZ FALSZYWY EMAIL

PODSZYWANIE SIĘ PODSZYWANIE SIE POD INNE OSOBY I INSTYTUCJE W CELU UZYSKANIA KORZYŚCI FINANSOWYCH WYSYŁANIE FAŁSZYWEGO E-MAILA SCAMER PODAJE SIĘ ZA PRACOWNIKA BANKU POD ZNANE FIRMY W SIECI OSOBA PRZEDSTAWIAJĄCA SIĘ NA PRZYKŁAD JAKO PRACOWNIK BANKU CZY INNY INSTYTUCJI W CELU WYŁUDZENIA PIENIĘDZY PODSZYWANIE SIĘ POD INNA OSOBĘ ATAKI MAILOWE LUB SMSOWE PODSZYWAJĄCE SIĘ POD POPULARNE USŁUGI UZYSKIWANIE DOSTĘPU DO POŁĄCZEŃ TELEFONICZNYCH BEZ ZGODY WŁAŚCICIELA RODZAJ CYBERATAKU PRÓBA WYSYŁANIE FAŁSZYWEGO EMAILA ALBO SMS

ZBIERANIE INFORMACJI NIE BARDZO ROZUMIEM POJĘCIE, TYLKO LEKKO MI SIĘ GDZIEŚ OBIŁO O USZY PODAWANIE SIĘ ZA KOGOŚ KIM SIĘ NIE JEST WYŁUDZANIA DANYCH KART BANKOWYCH POPRZEZ WYŁUDZENIE LUB PODSZYWANIE SIĘ POD KOGOŚ WPYCHANIE NIEPOTRZEBNYCH INFORMACJI W CELU OSZUSTWO W KTÓRYM KTOŚ PODSZYWA SIĘ POD INNĄ OSOBĘ LUB FIRMĘ W CELU WYŁUDZENIA DANYCH, LUB ZAINFEKOWANIA CYBERATAK MOBIL SPAM WDEIGHJ NIE WIEM WYŁUDZENIA DANYCH CHAMSTWO O8SZUSTWO INTERNETOWYCH CYBERATAK CYBERATAK, PRÓBA WYŁUDZENIA INFORMACJI

METODA OSZUSTWA, W KTÓREJ PRZESTĘPCA PODSZYWA SIĘ POD INNĄ OSOBĘ LUB INSTYTUCJĘ W CELU WYŁUDZENIA POUFNYCH INFORMACJI, ZAINFEKOWANIA KOMPUTERA SZKODLIWYM OPROGRAMOWANIEM CZY TEŻ NAKŁONIENIA OFIARY DO OKREŚLONYCH DZIAŁAŃ OSZUSTWO HGFDSASDFHJKLLIKJGJDSASDWHJ OSZUSTWO ZWIĄZANE Z WYŁUDZENIEM HASEŁ DO KONT, LUB Z INSTALACJĄ WIRUSÓW USŁUGĄ KTOŚ KTO SIĘ PODSZYWA POD INNĄ OSOBĘ W CELU WYŁUDZENIA POUFNYCH INFORMACJI PODESŁANIE FAŁSZYWEGO

LINKU I PODSZYWANIE SIĘ POD ZNANĄ INSTYTUCJĘ NĘKANIE REKLAMAMI I PROŚBAMI O ZALOGOWANIE SIĘ NA KONTO BANKOWE OSZUKIWANIE NIE WIEM WYŁUDZENIE DANYCH POPRZEZ FAŁSZYWE LINKI FAŁSZYWA INFORM ZŁOWIENIE OFIARY W CELU ZAINFEKOWANIA KOMPUTERA WIRUSEM LUB NAKŁONIENIA DO SZKODLIWYCH DZIAŁAŃ PHISHING TO RODZAJ CYBERATAKU, PODCZAS KTÓREGO CYBERPRZESTĘPCA PRÓBUJE WYŁUDZIĆ OD OFIARY POUFNE INFORMACJE KOJARZY MI SIĘ TO Z RYBAMI NIEWIEM WYŁUDZANIE BĄDŹ WYKRADANIE DANYCH NP. DOWÓD, NR KARTY KREDYTOWEJ, PESEL PRUBĄ WYŁUDZENIA DANYCH, PIENIĘDZY PRZEZ STOSOWANIE FAŁSZYWYCH LINKÓW Z GROŹNYM OPROGRAMOWANIEM FAŁSZYWE LINKI PRZESYŁANE NA POCZTĘ MAILOWĄ LUB SMS-EM MAILE WYGLĄDAJĄCE NA WIARYGODNE ALE PRÓBUJĄCE WYŁUDZIĆ INFORMACJE OSZUSTWO, W KTÓREJ KTOŚ PODSZYWA SIĘ POD INNĄ OSOBĘ W CELU WYŁUDZENIA DANYCH LUB NAKŁONIENIA DO OKREŚLONYCH DZIAŁAŃ WYŁUDZANIE DANYCH PRZEZ INTERNET ZAŚMIECANIE POCZTY NIECHCIANYMI INFORMACJAMI WYŁUDZANIEM DANYCH GDY KTOŚ CELOWO UŻYWA BŁĘDNEGO LINKA HTML, KTÓRY PROWADZI NIE DO OFICJALNEJ STRONY USŁUGODAWCY, BANKU ALBO FIRMY, TYLKO DO NIC DOBREGO N

SPREPAROWANEJ WITRYNY ŁUDZĄCO PODOBNEJ DO ORYGINALNEJ KRADZIEŻ TOŻSAMOŚCI TAK NICZYM ŁOWIENIE FRAJERA PODSTAWIONEJ JEST TO OSOBA KTÓRA PODAJE SIĘ ZA OSOBĘ LUB INSTYTUCJE W CELU OSZUKANIA DANEJ OSOBY Z PIENIEDZY OSZUSTWO POPRZEZ WYSYŁANIE FAŁSZYWYCH LINKÓW DO STRON, OFICJALNA STRONA JEST BARDZO PODOBNA. W MAILU MOGĄ BYĆ LITERÓWKI, ZALACZNIKI Z WIRUSAMI OCHRONA DANYCH ZAPOMNIAŁEM ZNECANIE SIE NAD LUDZMI WYCIEK NASZYCH DANYCH OSOBISTYCH METODA OSZUSTWA PRZEZ KONTAKT NIE OSOBISTY HACKOWANIE ŚLEDZENIE STRON INTERNETOWYCH NACIĄGANIE NA NIECHCIANE RZECZY CYBERPRZESTĘPCA PRÓBUJE WYŁUDZIĆ OD OFIARY POUFNE INFORMACJE BRAK TFJ NAJPROSTSZY I JEDNOCZEŚNIE NAJPOPULARNIEJSZY RODZAJ CYBERATAKU

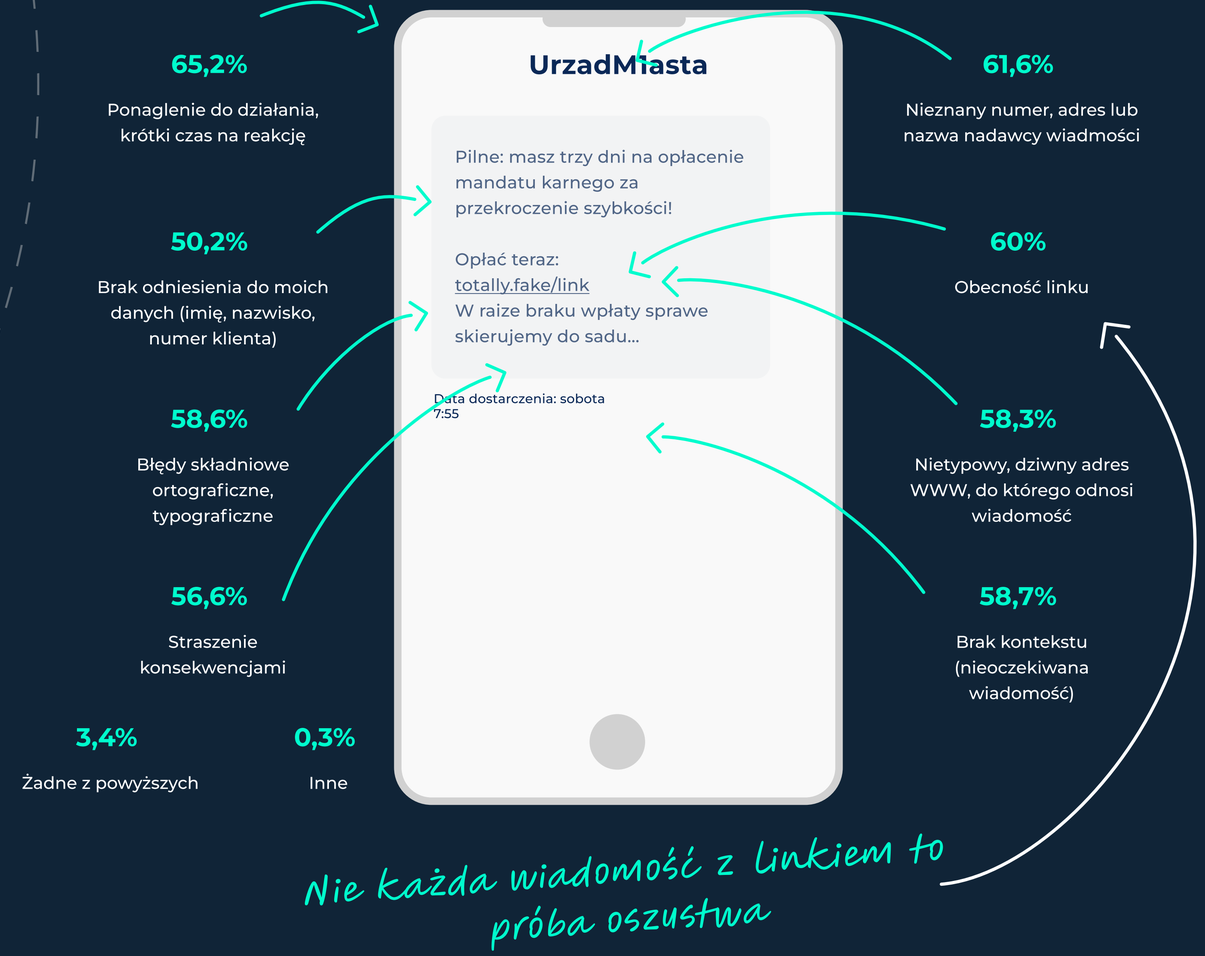
Jak rozpoznać **podejrzane treści?**

Anatomia podejrzanej wiadomości

Oszuści **żerują na nieuwadze, pośpiechu i przekonaniu, że większości konsekwencji można uniknąć**, reagując szybko.

Ponaglenie do działania, nieznajomy nadawca, brak kontekstu i straszenie konsekwencjami **to najczęściej wykorzystywane techniki**. Dlatego czytając wiadomość, zwracajmy uwagę na te elementy i starajmy się zachować spokój.

Wskaż elementy **wiadomości e-mail lub SMS**, które mogą wzbudzić Twoje **podejrzenie**. (wielokrotny wybór)



Linki w wiadomościach

Co sprawdzić przed kliknięciem w link?

- **Wcześniejszą komunikację z firmą** np. wyrażenie zgody na komunikację, zapis do newslettera lub klubu lojalnościowego
- Poprawność adresu www – **porównaj z adresem firmy, urzędu** lub instytucji
- **Przeczytaj wiadomość** ponownie za 5-10 minut i sprawdź, czy wywołuje takie same emocje
- W razie wątpliwości **skontaktuj się z oficjalną infolinią,** aby potwierdzić komunikat

Zaznacz, kiedy **klikasz w link w wiadomości** e-mail lub SMS. (wielokrotny wybór)

54,2%
Gdy znamy nadawcę

52,3%
Gdy spodziewam się danej wiadomości

28,9%
Gdy wcześniej wyraziłam/em zgodę na otrzymanie

28,5%
Gdy adres WWW nie wzbudza podejrzeń

15,7%
Gdy wiadomość dotyczy statusu moich ważnych spraw np. rachunków

11%
Gdy treść wiadomości mnie zainteresuje

5,8%
Gdy brak reakcji wiąże się z negatywnymi konsekwencjami

5,6%
Gdy komunikat wymaga szybkiej reakcji, pilnego działania

3,8%
Gdy sprawę można szybko zrealizować, mieć ją szybko z głowy

14,5%
Żadne

0,2%
Inne

Komentarz

Od wielu lat zajmuje się propagowaniem wiedzy na temat bezpieczeństwa danych osobowych. Autor licznych wystąpień medialnych, w których tłumaczy aktualne sposoby działania oszustów i cyberprzestępców oraz radzi, jak unikać negatywnych konsekwencji kradzieży danych osobowych.

Bartłomiej Drozd
Ekspert serwisu **ChronPESEL.pl**

Ekspert raportu

Konsekwencje phishingu mogą być różne, wszystko zależy od tego, czy rozpoznamy go na wczesnym etapie, czy ujdzie on przestępcom płazem. Hakerom przede wszystkim zależy na zdobyciu od nas danych albo pieniędzy. Warto więc mieć na uwadze wszystkie wiadomości SMS czy e-mail próbujące wmówić nam, że mamy nieopłaconą przesyłkę. **To samo tyczy się wiadomości, które mówią o nieuzupełnionym koncie i braku pewnych danych**. To jedne z popularniejszych sposobów na wyłudzenia, na które niestety w przypływie chwili często dajemy się nabrać. Jeżeli udostępnimy takie dane, a dopiero później zauważymy, że mogła to być fałszywa strona czy wiadomość od przestępcy – **możemy jeszcze działać i uchronić się przed większą stratą**. Warto monitorować nasz numer PESEL, jeśli go podawaliśmy, a jeśli wpisywaliśmy tam numer naszej karty płatniczej – koniecznie musimy ją zastrzec w banku. Jeżeli dostaliśmy już wiadomość e-mail, przyjrzyjmy się adresowi, z jakiego została wysłana.

Nie zwracajmy uwagi na szatę graficzną danej wiadomości, ponieważ przestępcom coraz lepiej wychodzi kopiowanie oryginalnych stron, pod jakie się podszywają. Porównajmy adres e-mail z tymi dostępnymi na stronie internetowej przedsiębiorstwa. **Jeżeli mowa zaś o wiadomościach SMS, koniecznie sprawdźmy link, który zawsze jest dołączony do próby wyłudzenia.** Nie klikajmy w niego, ale porównajmy z wiarygodnymi źródłami. Jeżeli jest to np. usługa kurierska, wyszukajmy w wyszukiwarce stronę internetową kuriera i sprawdźmy jej oryginalny odnośnik. W przypadku kontaktu telefonicznego, najlepiej się rozłączyć i samemu zadzwonić pod numer podany na stronie.

Komentarz cd.

Od wielu lat zajmuje się propagowaniem wiedzy na temat bezpieczeństwa danych osobowych. Autor licznych wystąpień medialnych, w których tłumaczy aktualne sposoby działania oszustów i cyberprzestępców oraz radzi, jak unikać negatywnych konsekwencji kradzieży danych osobowych.

Bartłomiej Drozd
Ekspert serwisu **ChronPESEL.pl**

Ekspert raportu

Cyberprzestępcy, którzy chcą wyłudzić od nas dane osobowe albo pieniądze, najczęściej mają już nasze dane kontaktowe (numer telefonu, adres e-mail). To, można powiedzieć, połowa ich sukcesu. Czasami zdarza im się posiadać również informacje mniej znaczące, jak na przykład bank, z którego na co dzień korzystamy czy usługi pocztowe, **z których korzystaliśmy w niedawnym czasie**. Dzieje się tak najczęściej ze względu na wycieki danych z baz tych instytucji i firm.

Niestety to jest coś, na co nie mamy bezpośredniego wpływu. Możemy jednak się ustrzec przed próbami wyłudzenia, zachowując nadzwyczajną ostrożność, czytając wiadomości czy odbierając telefony. Tacy przestępcy często posiadają też inne dane na nasz temat, które pomagają im uśpić naszą czujność. **W końcu nie każdy wie, jaka jest nasza dokładna data urodzenia**, czy w jakim sklepie online robiliśmy ostatnio zakupy. A właśnie na takie informacje powołują się hakerzy, próbując wyłudzić od nas pozostałe dane.

Rada #1

Jak bronić się przed
oszustwami internetowymi?

Czytaj uważnie
otrzymywane **komunikaty!**

Jak **zabezpieczamy się** przed **oszustwami** internetowymi?

24 ● Wskaż wszystkie kanały komunikacji z firmami, które uważasz za bezpieczne.

25 ● Zaznacz wszystkie sposoby, które wykorzystujesz, aby zabezpieczyć się przed oszustwami internetowymi.

26 ● Wskaż wszystkie sposoby zabezpieczeń, z których korzystasz.

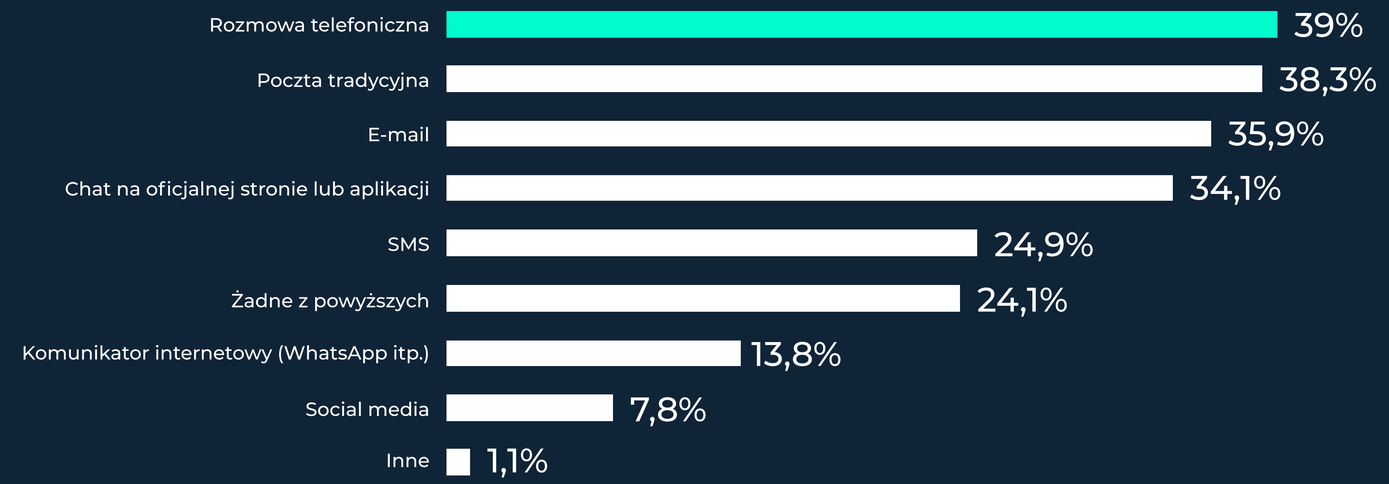
27 ● Rada #2

Bezpieczne kanały komunikacji

Według **39% respondentów** rozmowy telefoniczne są bezpiecznym kanałem komunikacji z firmami i urzędami.

Niemalże **co czwarty** ankietowany wskazał w tej roli wiadomości tekstowe.

Wskaż **wszystkie kanały komunikacji** z firmami, które uważasz za bezpieczne. (wielokrotny wybór)

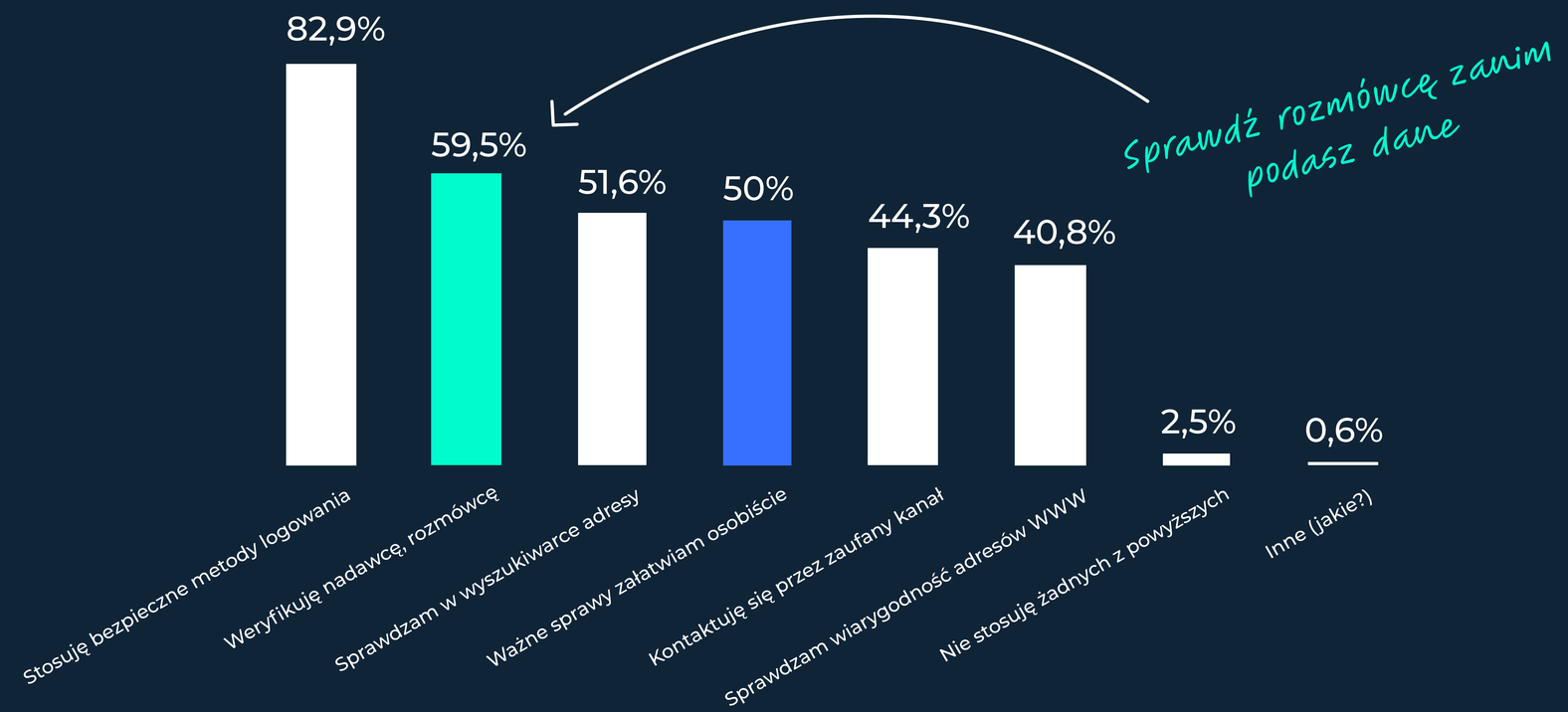


Metody zabezpieczeń przed atakami

Świadomość zagrożeń wynikających z niekontrolowanej komunikacji jest silna, **co drugi weryfikuje tożsamości** rozmówcy, nadawcy oraz adres czy numer.

Co drugi ankietowany woli ważne sprawy załatwiać osobiście w urzędzie lub placówce firmy.

Zaznacz **wszystkie sposoby**, które wykorzystujesz, aby **zabezpieczyć się przed oszustwami** internetowymi. (wielokrotny wybór)



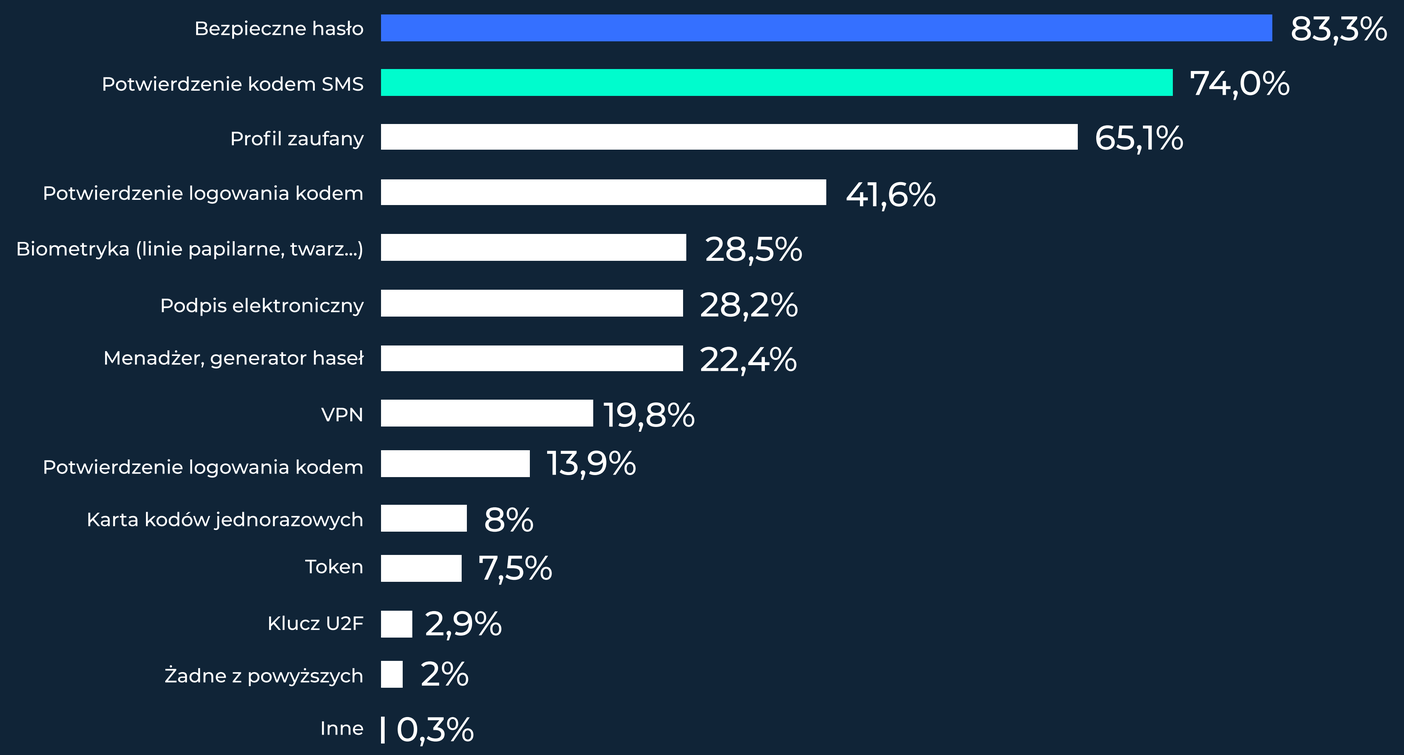
Bezpieczeństwo logowania

Aż 74% ankietowanych uważa, że wiadomości SMS z kodem zwiększają **bezpieczeństwo logowania.**

Jakie powinno być bezpieczne hasło?

- **Unikalne** – jedno hasło do jednego serwisu, usługi
- **Długie** – przynajmniej 12 znaków
- **Skomplikowane** – korzystaj z menadżerów do generowania i przechowywania losowych haseł
- **Niezwiązane z datą urodzenia**, imieniem bliskich ani innymi danymi, które łatwo powiązać z użytkownikiem

Wskaż **wszystkie sposoby zabezpieczeń**, z których korzystasz. (wielokrotny wybór)



Rada #2

Jak bronić się przed
oszustwami internetowymi?

Pomyśl zanim podasz dane

Jak reagujemy na próby ataków i **podejrzane treści**?

Reakcja na podejrzane treści

Gdzie zgłaszać podejrzane wiadomości?

- SMS przekaż do **CERT** na numer**: 8080**
- Incydenty zgłaszaj do **CERT: https://incydent.cert.pl**
- **Ostrzeż rodzinę oraz znajomych o niebezpieczeństwie**

Zaznacz wszystko, co robisz, **gdy otrzymujesz fałszywą wiadomość** e-mail lub SMS. (wielokrotny wybór)

57,6%
Natychmiast usuwam wiadomość

45,9%
Ostrzegam rodzinę i znajomych

25,4%
Szukam informacji o zdarzeniu i dalszym postępowaniu

16%
Kontaktuję się z podmiotem, pod którego podszywa się wiadomość

15,6%
Zgłaszam zdarzenie operatorowi komórkowemu

13,9%
Zgłaszam zdarzenie na stronie CERT czy podobnej

10,6%
Zgłaszam zdarzenie na policję

8%
Zgłaszam zdarzenie portalom typu Niebezpiecznik czy podobnym

7,6%
Nic nie robię

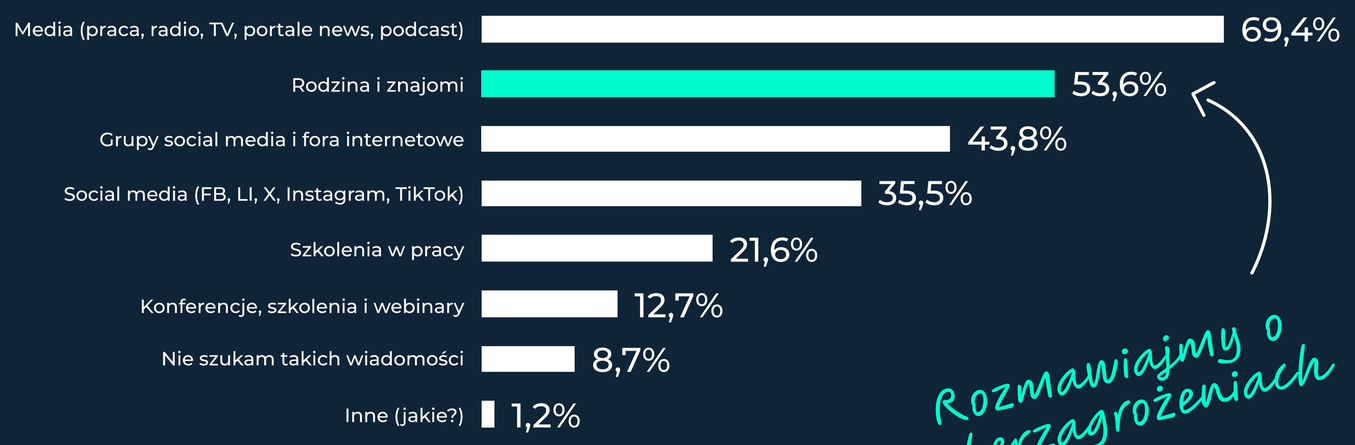
0,2%
Inne

Źródła wiedzy o cyberzagrożeniach

Rozprzestrzenianie niesprawdzonych, fałszywych danych czy relacji jest poważnym zagrożeniem. **Generuje szum informacyjny, pogłębia podziały**, a także rozmywa wartość prawdziwych wiadomości. A na tym wszystkim zależy oszustom.

Zawsze **weryfikuj źródło** i treść informacji, które do Ciebie trafiają.

Zaznacz wszystkie źródła, z których **zdobywasz wiedzę na temat aktualnych zagrożeń** bezpieczeństwa w sieci. (wielokrotny wybór)



Komentarz

Praktyk i entuzjasta rynku IT, ponad 20 lat doświadczenia na stanowiskach związanych z infrastrukturą i bezpieczeństwem IT – od administratora sieci i usług u operatorów telco do członka zarządu polskiego producenta systemów PAM (Fudo). Obecnie rozwija własne rozwiązanie do testów funkcjonalnych – TestCLIX i jednocześnie prowadzi zespół najlepszych inżynierów IT security w kraju 😉 będąc CTO w 4Prime. Entuzjasta Linuxa i starej szkoły IT. Prywatnie meloman, basista i miłośnik jazdy na rowerze elektrycznym.

Michał Malanowicz
Technical Team Leader, IT Security Consultant,
4Prime sp.z o.o.
Grupa 4Prime IT Security

O istotności komunikacji nikomu nie trzeba mówić. Wymiana informacji to istota działania każdego z nas, każdej firmy i każdej instytucji. **W dzisiejszych czasach coraz częściej spotykamy się z kanałem komunikacji elektronicznej**. Do poczty elektronicznej na masową skalę dołączyły różnego rodzaju “bezpieczne" komunikatory, każdy zna aplikacje typu WhatsApp czy Messenger, a także Zoom czy Teams. Narzędzi jest na rynku niezliczona ilość i każdy program stara się oferować coś unikalnego, czym przyciąga kolejnych użytkowników. Niektóre walczą ceną, inne - będąc pozornie darmowe, wysyłają dane o użytkowniku na serwery albo stanowią bramę dla innego oprogramowania szpiegowskiego.

Wszystko wskazuje na przykład, że **program do podsłuchu Pegasus - wykorzystywał do zainstalowania się luki w programie WhatsApp**. Które zatem programy uznaje się za bezpieczne? Tu warto zaufać specjalistom od bezpieczeństwa IT.

Z pewnością do takich rozwiązań należy Microsoft Teams czy biurowe pakiety Google i Apple. Z drugiej strony rozwiązania darmowe wiążą się prawie zawsze z udostępnieniem części danych o korespondencji firmom trzecim w celach statystycznych i marketingowych. W dzisiejszym świecie nie ma nic za darmo.

Cyfrowe kanały komunikacji powinny być też odpowiednio zabezpieczone przed niepowołanym dostępem. Wskazane jest **korzystanie z rozwiązań, które wykorzystują mechanizmy MFA** (multi factor authentication).

Komentarz cd.

Praktyk i entuzjasta rynku IT, ponad 20 lat doświadczenia na stanowiskach związanych z infrastrukturą i bezpieczeństwem IT – od administratora sieci i usług u operatorów telco do członka zarządu polskiego producenta systemów PAM (Fudo). Obecnie rozwija własne rozwiązanie do testów funkcjonalnych – TestCLIX i jednocześnie prowadzi zespół najlepszych inżynierów IT security w kraju 😉 będąc CTO w 4Prime. Entuzjasta Linuxa i starej szkoły IT. Prywatnie meloman, basista i miłośnik jazdy na rowerze elektrycznym.

Michał Malanowicz
Technical Team Leader, IT Security Consultant,
4Prime sp.z o.o.
Grupa 4Prime IT Security

To minimum i w dzisiejszych czasach jest całkiem wygodne – **dodatkowym składnikiem uwierzytelnienia może być dziś SMS**, aplikacja na telefon, ale też dane biometryczne jak np. odcisk palca.

Korzystanie nawet z najlepszych form komunikacji cyfrowej nie zapewni skutecznej ochrony przed oszustwami internetowymi. To zupełnie oddzielna kategoria problemów i choć gdy komunikacja jest bezpieczna to na jej końcu **zawsze pozostaje najsłabsze ogniwo - człowiek**. Jesteśmy podatni na różnego rodzaju komunikaty o promocjach (wymagających podania danych karty), problemach z dostarczeniem przesyłki kurierskiej (również kierującej do fałszywej strony z płatnościami), problemami z kontem bankowym czy inne – zawierające równie wymyślne historyjki, które czasem trafiają na podatny grunt. Tu działa statystyka, każdy może mieć gorszy dzień, być zdezorientowany czy po prostu kliknąć przez przypadek w nieodpowiednie pole np. pozwól, a nie anuluj.

Najlepszą ochroną jest okresowe szkolenie z metod jakimi posługują się hakerzy i świadomość oczywistych rzeczy, takich jak np. że bank nigdy nie kontaktuje się z klientami telefonicznie w celach związanych z dostępem do konta albo że nie klika się w linki z poczty kierujące do bramek płatniczych, nawet jeśli zawierają treść identyczną do comiesięcznych opłat za telefon czy prąd. Zawsze w takich przypadkach logujemy się do eBok podmiotu świadczącego usługi dla nas i dopiero stamtąd dokonujemy płatności.

Komentarz cd.

Praktyk i entuzjasta rynku IT, ponad 20 lat doświadczenia na stanowiskach związanych z infrastrukturą i bezpieczeństwem IT – od administratora sieci i usług u operatorów telco do członka zarządu polskiego producenta systemów PAM (Fudo). Obecnie rozwija własne rozwiązanie do testów funkcjonalnych – TestCLIX i jednocześnie prowadzi zespół najlepszych inżynierów IT security w kraju 😉 będąc CTO w 4Prime. Entuzjasta Linuxa i starej szkoły IT. Prywatnie meloman, basista i miłośnik jazdy na rowerze elektrycznym.

Michał Malanowicz
Technical Team Leader, IT Security Consultant,
4Prime sp.z o.o.
Grupa 4Prime IT Security

Jeśli podejrzewamy, że dostaliśmy fałszywą wiadomość w pracy to najlepiej ją po prostu skasować i zgłosić sprawę do działu bezpieczeństwa lub IT w firmie – szczególnie, jeśli zjawisko powtarza się.

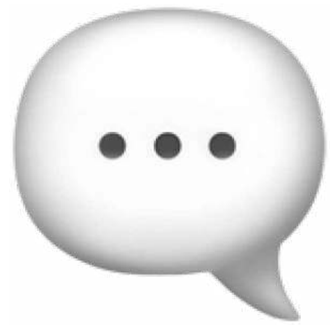
Odpowiednie kroki zostaną podjęte praktycznie natychmiast i będą one polegały na **filtrowaniu podobnych wiadomości, blokowaniu nadawców i numerów**, z których pochodzą wiadomości, modyfikacji polityk bezpieczeństwa a także współpracy z operatorami i dostawcami usług telekomunikacyjnych.

Sami jako konsumenci możemy relatywnie niewiele, choć w internecie jest już kilka stron identyfikujących np. numery telefoniczne bramek wykorzystywanych przez hakerów czy strony opisujące metody oszustwa na telefon. Warto doszkalać się we własnym zakresie i regularnie korzystać z uznanych stron jak niebezpiecznik.pl czy sekurak.pl. Informacji związanych z bezpieczeństwem dostarcza również policja.

Rada #3

Jak bronić się przed
oszustwami internetowymi?

Rozmawiaj i dziel się doświadczeniem



Podsumowanie raportu

Szymon Sidoruk to absolwent informatyki na Politechniki Warszawskiej, przez całą karierę zawodową związany z cyberbezpieczeństwem w CERT Polska. Od początku zajmuje się tematyką rozpoznawania zagrożeń oraz edukacji użytkowników.

Szymon Sidoruk
Specjalista ds. Analizy Zagrożeń
CERT Polska

CERT Polska działa w NASK od 1996 w celu monitorowania zagrożeń i reagowania na zgłaszane incydenty. Od 2018 roku pełni rolę CSIRT NASK w ramach Krajowego Systemu Cyberbezpieczeństwa. Każdego dnia aktywnie **uczestniczymy w rozwijaniu świadomości w obszarze cyberbezpieczeństwa**, angażujemy się w projekty podnoszące wiedzę i kompetencje. Raport Bezpieczeństwo Cyfrowe Polaków rzuca światło na aktualne wyzwania w zakresie korzystania z internetu. Zaprezentowane wnioski mogą być pomocne dla skuteczniejszego budowania świadomości wśród użytkowników.

W ciągu ostatnich lat zauważalny jest dynamiczny rozwój cyfryzacji usług w Polsce. Dotyczy to zarówno sektora publicznego, jak i komercyjnego. Jeszcze nie tak dawno temu nie przeszłoby nam przez myśl, że Urząd Skarbowy czy Policja skomunikuje się z nami SMS-em. Dzisiaj na każdym kroku mierzymy się z takimi wiadomościami – dostajemy maila lub SMS-a o rozpoczęciu płatności, o przyjęciu paczki przez kuriera czy ponaglenie za nieopłacone rachunki.

W sklepie o wiele szybciej i sprawniej płaci się kartą, a zakupy w internecie są jeszcze przyjemniejsze, bo przecież nawet nie musimy wychodzić z domu. Przed chwilą przeglądaliśmy media społecznościowe i właśnie płacimy za przedmiot, który podpowiedziała nam reklama. Za chwilę odczytamy potwierdzenie płatności i zobaczymy na mailu zaległy rachunek za internet.

Operujemy na schematach, utartych scenariuszach. Kiedy widzimy stronę pośrednika płatności (a przynajmniej tak wyglądającą) od razu wiemy, co wpisać. Ponad **90% SMS-ów jest odczytywanych w ciągu 15 min od doręczenia**, a czas kliknięcia w link od wyświetlenia wiadomości to kwestia sekund. Z tego powodu najważniejsza jest pamięć o tym, że telefon to wyłącznie narzędzie. Kluczowe jest wyrobienie nawyku weryfikowania każdej informacji, która się na nim wyświetla.

Podsumowanie raportu cd.

Rada #1

Czytaj uważnie otrzymywane komunikaty

Widząc skalę procesów związanych z cyfryzacją naszego życia zupełnie nie dziwi, że 75,4% badanych otrzymało podejrzane treści SMS-em. W odpowiedzi na ten problem prowadzimy numer 8080, na który można przekazać niezmienioną treść takiej wiadomości.

Warto podkreślić, że aż **65,2% osób zwraca uwagę na próbę wywołania presji czasu**, a **56,6% wskazuje straszenie konsekwencjami**. Właśnie dlatego drugim dobrym nawykiem jest niereagowanie na wiadomości, które wywołują w nas emocje. Warto **poczekać kilka minut i przeczytać ponownie**, zobaczyć czy wiadomość jest dla nas tak samo wiarygodna. Nawet jeżeli się początkowo byliśmy gotowi zaufać nadawcy, to jest szansa, że do czasu ponownego odczytania SMS-a, witryna z linku zostanie zablokowana przez Listę ostrzeżeń CERT Polska. Na stronie https://lista.cert.pl/ można sprawdzić, czy nasz dostawca internetu z niej korzysta.

Z tego powodu trzeba poznać kilka podstawowych zasad, których znajomość może nas ochronić. Jeżeli jesteśmy w stanie rozpoznać podrobiony artykuł na podstawie metki, to jeśli będziemy wiedzieć gdzie szukać, rozpoznamy również fałszywą stronę, dla której domena jest tą przysłowiową metką. Warto też **zwracać uwagę na bezpieczeństwo innych mechanizmów**, z których korzystamy np. dane karty kredytowej wykorzystywane są wyłącznie do płatności, jeżeli ktoś chce je od nas uzyskać pod pretekstem przelania nam pieniędzy, to możemy łatwo rozpoznać oszustwo.

Zaskakujące, że tylko 34,1% respondentów uważa czat na oficjalnej stronie lub w aplikacji za bezpieczny kanał komunikacji. Jest to tak naprawdę jedyny w pełni bezpieczny sposób na komunikację, aby bez ryzyka korzystać z tej formy komunikacji, **trzeba nauczyć się rozpoznawać prawidłową stronę** na podstawie domeny.

Podsumowanie raportu cd.

Rada #2

Pomyśl zanim podasz dane

To kolejny aspekt potrzebny do zapewnienia bezpieczeństwa, bo korzystanie z komputera to też umiejętność.

Ważnym elementem zapewnienia sobie bezpieczeństwa jest **korzystanie z wieloskładnikowego uwierzytelnienia** tam, gdzie to możliwe. Automatycznie chroni nas to przed atakami, które pozyskują same dane logowania. W takim wypadku nawet po złamaniu hasła nasze konto będzie chronione.

Warto korzystać też z **menadżerów haseł**, rozwiązuje to problem z zapamiętywaniem, a jednocześnie pozwala na używanie unikalnego hasła dla każdej usługi – co dla odmiany chroni przed rozległymi skutkami wycieku danych. Menadżery posiadające opcję uzupełniania pomogą nam także nauczyć się rozpoznawania phishingu, ponieważ wiążą dane logowania z domeną, na której stworzyliśmy konto.

Najbardziej zaniedbywaną wg mnie radą jest **zwracanie uwagi na komunikaty przy operacjach bankowych**. W przypadku oszustw z płatnościami może to nam uratować oszczędności życia. Sposoby na wyprowadzenie pieniędzy są dwa. Pierwszym jest ustawienie odbiorcy zdefiniowanego, drugim natomiast proszenie o wiele kodów operacji pod pretekstem wpisania błędnego kodu. Niezależnie od metody używanej przez przestępców w SMS-ie lub aplikacji wyświetli się typ operacji i kwota. Jeżeli płacimy złotówkę za prąd, a dostajemy powiadomienie o ustawieniu odbiorcy zdefiniowanego lub przelewie 3000 zł, to mamy pewność, że ktoś właśnie próbuje nas oszukać.

Edukacja w zakresie rozpoznawania i przeciwdziałania oszustwom w sieci to działanie wielowymiarowe. Potrzebujemy chęci użytkowników do pozyskiwania nowej wiedzy, jak i doskonalszych, bardziej zrozumiałych komunikatów np. w naszych social mediach.

Podsumowanie raportu cd.

Rada #3

Rozmawiaj i dziel się doświadczeniem

Warto pamiętać, że w razie jakichkolwiek problemów z rozpoznaniem zagrożenia można się **zwrócić do CERT Polska** korzystając z instrukcji na https://incydent.cert.pl/.

Ale udzielanie pomocy w rozpoznaniu to jeden aspekt naszej pracy, drugim jest przeciwdziałanie zagrożeniom np. w postaci wspomnianej Listy ostrzeżeń. Do tego potrzebujemy też zgłoszeń od osób, które rozpoznają zagrożenia samodzielnie Z tego powodu chcielibyśmy, żeby w kolejnej edycji badania znacznie więcej niż 13,9% osób zadeklarowało zgłaszanie zagrożeń na stronie CERT Polska czy podobnej. Godne pochwały są natomiast deklaracje **aż 45,9% respondentów, którzy ostrzegają znajomych i rodzinę**.

Podsumowując, raport poprawnie wskazuje, że edukacja oraz **wymiana informacji to najlepsze zabezpieczenie** przed próbami nadużyć opartych na phishingu oraz innymi formami ataków. Budowanie wzajemnej odpowiedzialności społecznej za nasze wspólne przecież bezpieczeństwo jest kluczem do sukcesu.

Szymon Sidoruk – CERT Polska

Partnerzy

Dzięki za uwagę!

SMSAPI
Powered by LINK Mobility

Porozmawiajmy

mpr@smsapi.pl

Śledź nas