WARSZAWSKI INSTYTUT BANKOWOŚCI

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

RAPORT

CYBERBEZPIECZNY PORTFEL

publikacja
Warszawskiego Instytutu Bankowości pod patronatem **Związku Banków Polskich**

ZWIĄZEK BANKÓW POLSKICH

BANKOWCY DLA EDUKACJI
program sektorowy

edycja V
październik 2024

SPIS TREŚCI

	O RAPORCIE „CYBERBEZPIECZNY PORTFEL”	3
ROZDZIAŁ I	WYBRANE LICZBY Z BADANIA „POSTAWY POLAKÓW WOBEC CYBERBEZPIECZEŃSTWA”	5
ROZDZIAŁ II	CYFROWY PORTFEL A CYBERBEZPIECZEŃSTWO W BANKOWOŚCI	8
ROZDZIAŁ III	CYFROWY ŚWIAT: ZAGROŻENIA I ZABEZPIECZENIA	15
ROZDZIAŁ IV	NOWE TECHNOLOGIE	28
ROZDZIAŁ V	EDUKACJA, EDUKACJA I JESZCZE RAZ EDUKACJA	36
ROZDZIAŁ VI	ABC CYBERBEZPIECZEŃSTWA – TOP 10 ZASAD CYFROWEGO BEZPIECZEŃSTWA	40
	ŹRÓDŁA I AUTORZY RAPORTU	45
	O PROJEKCIE EDUKACYJNYM „BEZPIECZEŃSTWO W CYBERPRZESTRZENI”	46

O RAPORCIE

RAPORT „CYBERBEZPIECZNY PORTFEL” TO CYKLICZNA PUBLIKACJA WARSZAWSKIEGO INSTYTUTU BANKOWOŚCI WYDAWANA OD 2016 R. POD PATRONATEM ZWIĄZKU BANKÓW POLSKICH, KTÓRA PRZYBLIŻA TRENDY POSTAW SPOŁECZNYCH W CYFROWYM ŚWIECIE ZE SZCZEGÓLNĄ UWAGĄ NA KWESTIE BEZPIECZEŃSTWA I ZAGROŻEŃ.

W Polsce, podobnie jak na całym świecie, obserwujemy wyraźne odstępowanie od tradycyjnych form płatności na rzecz metod bezgotówkowych. Raport wskazuje, że Polacy są coraz bardziej otwarci na nowe technologie: nie tylko coraz chętniej płacą zbliżeniowo smartfonem czy z użyciem BLIK-a, ale również korzystają z tzw. urządzeń ubieralnych typu smartwatch i coraz bardziej interesują się technologią biometryczną czyli np. autoryzowaniem transakcji za pomocą odcisku palca.

Cyfryzacja różnych usług sprawia, że ich użytkownicy mogą zetknąć się z różnymi działaniami cyberprzestępców – współcześni przestępcy asymilują się ze cyfrowym światem i szukają coraz to nowych metod oszustw w sieci. Raport przedstawia całą listę takich zagrożeń, a na szczycie tego zestawienia znajduje się tzw. phishing, czyli zdobywanie poufnych informacji w celu wyłudzenia pieniędzy. Ponadto, publikacja nawiązuje także do tematu wykorzystania sztucznej inteligencji oraz stosunku Polaków wobec jej użytkowania, a także zwraca uwagę na rosnący problem dezinformacji, w tym właśnie z użyciem AI.

Raport ma na celu nie tylko dostarczyć ważnych danych, ale także być źródłem wiedzy w zakresie właściwych postaw w obszarze cyberbezpieczeństwa, stąd zawiera także zestawienie podstawowych porad, które zwiększą bezpieczeństwo w sieci każdego z nas i naszego portfela.

Zachęcamy do szczegółowego zapoznania się z raportem oraz dzielenia się wiedzą, danymi i wnioskami zdobytymi po tej lekturze!

MICHAŁ POLAK,
WICEPREZES FUNDACJI
WARSZAWSKI INSTYTUT BANKOWOŚCI

Badanie „Postawy Polaków wobec cyberbezpieczeństwa 2024” i raport „Cyberbezpieczny Portfel” zrealizowano w ramach projektu edukacyjnego WIB „Bezpieczeństwo w Cyberprzestrzeni”, który jest częścią Programu sektorowego „Bankowcy dla Edukacji”.

Raport „Cyberbezpieczny Portfel” zawiera wyniki badania „Postawy Polaków wobec cyberbezpieczeństwa 2024”, zleconego przez Fundację Warszawski Instytut Bankowości (WIB), a przeprowadzonego przez firmę badawczą SW Research. Badanie wykonano w formie ankiety online na reprezentatywnej próbie 1007 osób (Polek i Polaków) w wieku 18–50+.

Raport „Cyberbezpieczny Portfel” publikowany jest co dwa lata.

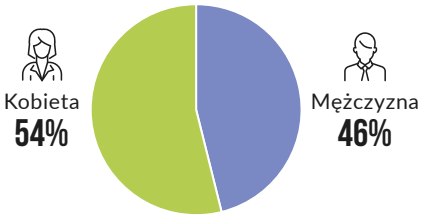
ROZDZIAŁ I

Wybrane liczby z badania „Postawy Polaków wobec cyberbezpieczeństwa”

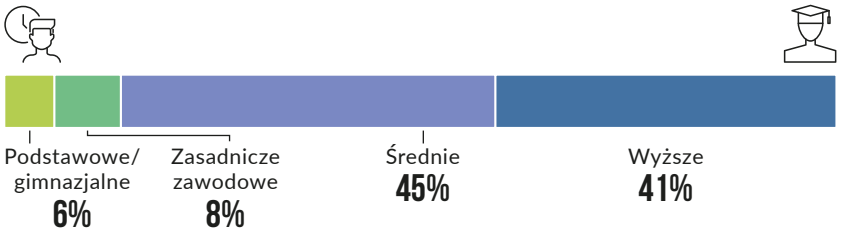
METRYCZKA BADANIA[1]

STRUKTURA DEMOGRAFICZNA BADANYCH

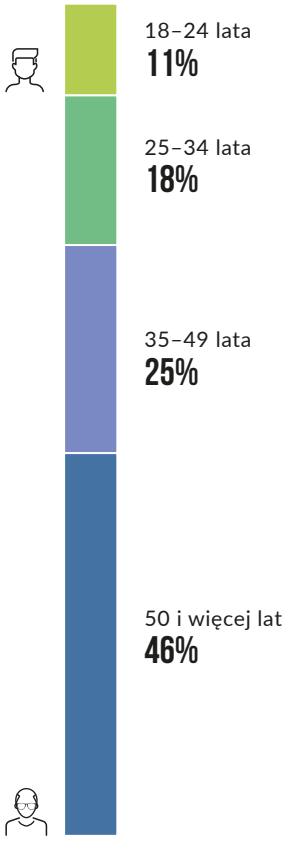
PŁEĆ



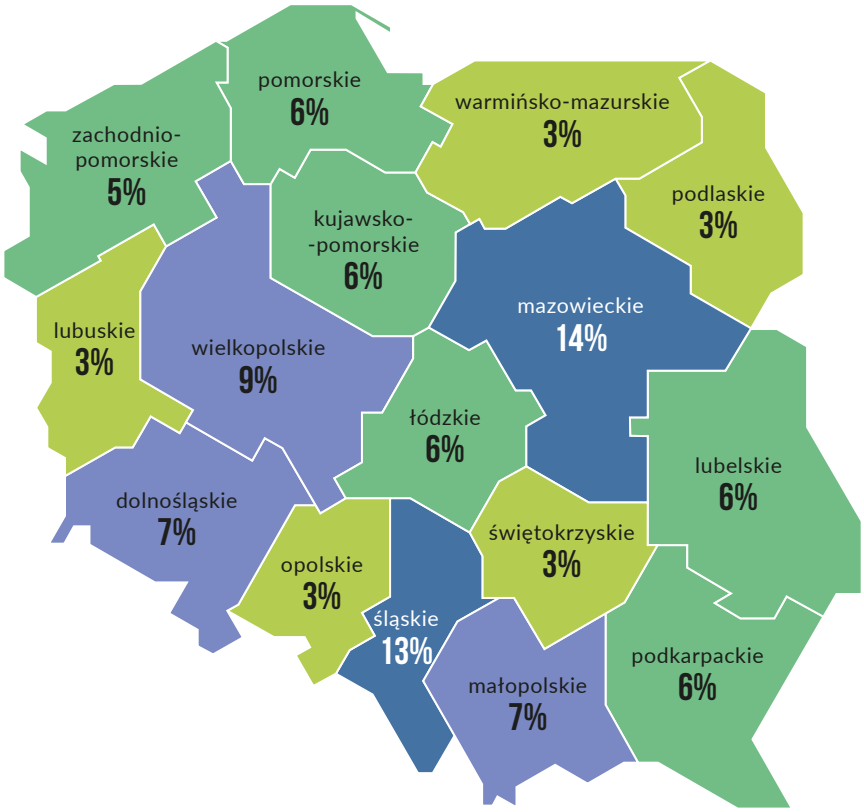
WYKSZTAŁCENIE



KATEGORIA WIEKOWA

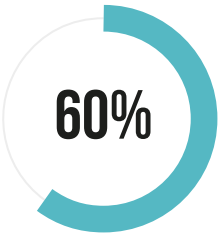


WOJEWÓDZTWO

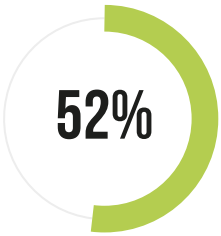


1/ W raporcie dane procentowe z badania „Postawy Polaków wobec cyberbezpieczeństwa" zostały stosownie zaokrąglone dla przejrzystości przekazu.

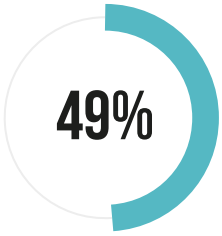
KLUCZOWE WNIOSKI I TRENDY



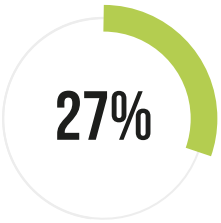
60% respondentów najbardziej obawia się, że w cyfrowym świecie zostaną wyłudzone ich dane,



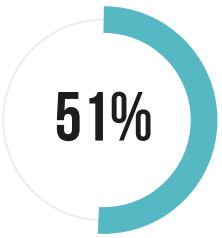
a 52% że pieniądze



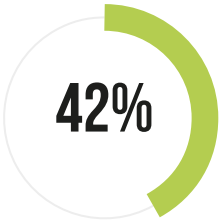
49% badanych uważa, że AI jest zarówno szansą, jak i zagrożeniem dla człowieka



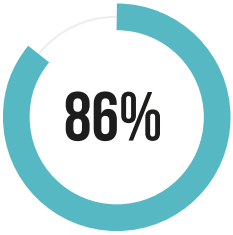
ale przeciwników AI jest prawie dwukrotnie więcej od zwolenników: 27% obawia się jej, a 14% uznaje ją za wsparcie



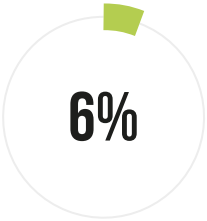
51% Polaków obawia się kradzieży tożsamości,



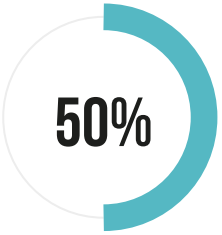
a 42% fake newsów i dezinformacji



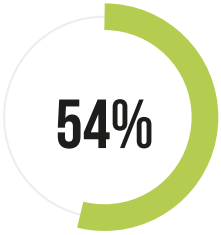
86% respondentów czuje się bezpiecznie korzystając z bankowości internetowej lub mobilnej,



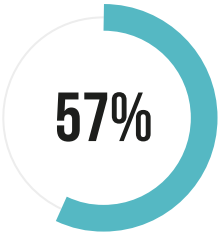
ale tylko 6% zdecydowanie czuje się bezpiecznie korzystając z Internetu



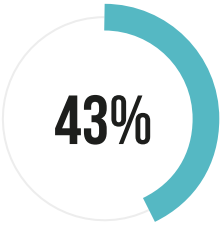
50% Polaków uważa, że odpowiedzialność za bezpieczeństwo finansowych usług cyfrowych spoczywa na bankach,



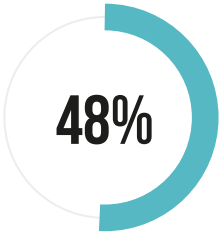
równocześnie 54% wskazuje banki za liderów cyberbezpieczeństwa



57% badanych korzysta z bankowości mobilnej używając smartfona

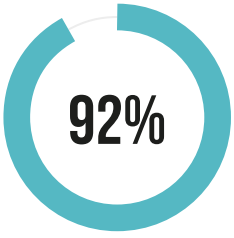


43% respondentów deklaruje chęć weryfikacji płatności odciskiem palca lub próbką głosu



48% Polaków posiada tylko orientację w temacie cyberbezpieczeństwa,

a 15% wie niewiele



92% uważa, że jest potrzeba edukowania społeczeństwa na temat cyberbezpieczeństwa!

ROZDZIAŁ II

Cyfrowy portfel a cyberbezieczeństwo w bankowości

CYFROWY PORTFEL I PŁATNOŚCI MOBILNE ZYSKUJĄ NA POPULARNOŚCI

Cyfryzacja usług na wielu płaszczyznach, w tym w finansach i bankowości jest już powszechnym trendem współczesnej rzeczywistości. Obecnie oprócz gotówki mamy również cyfrowe portfele, które z dekady na dekadę cieszą się coraz większą popularnością.

PORTFEL CYFROWY

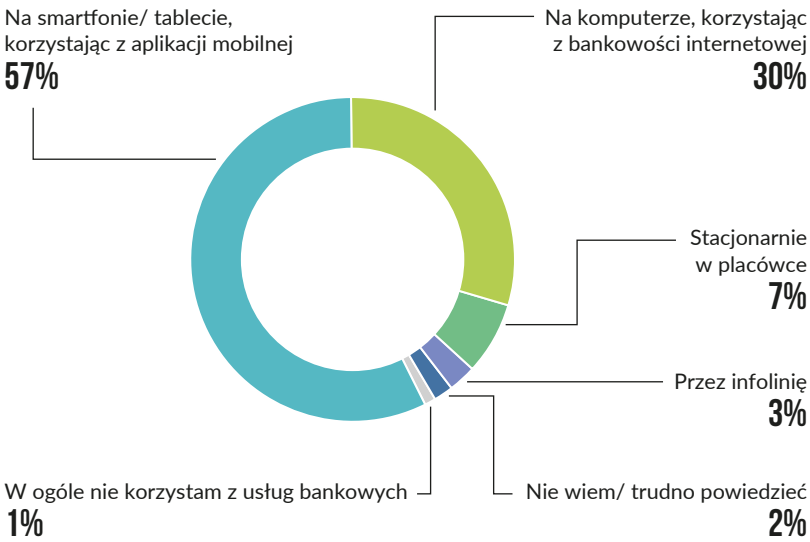
to odpowiednik tradycyjnego portfela, tyle że używanego w przestrzeni wirtualnej (tzw. pass-through digital wallet). Jednym z rodzajów portfeli cyfrowych są aplikacje używane na smartfonach albo portfele zainstalowane na tzw. urządzeniach ubieralnych (z ang. wearables), typu smartwatch/inteligentne zegarki, dzięki którym możemy dokonywać płatności zbliżeniowych w sklepie lub online.

źródło: VISA

Przykładowo, w I kwartale 2024 r. za pomocą mobilnych płatności zbliżeniowych przeprowadzono przeszło 385 mln transakcji. Najpopularniejsze cyfrowe portfele w Polsce to Google Pay oraz Apple Pay – liczba płatności takimi e-portfelami wzrosła w ciągu roku o ponad 100 mln[2]. Jak wynika z danych Fundacji Polska Bezgotówkowa, skala zmian jaka się wydarzyła na przestrzeni ostatnich trzech dekad jest ogromna – począwszy od plastikowych kart płatniczych, których w 1993 r. na polskim rynku było niespełna 50 tys., po ponad 10,8 mln kart podpiętych do cyfrowych portfeli płatniczych w 2023 roku[3].

Popularność płatności mobilnych w Polsce potwierdza także kluczowe dla tego raportu badanie Warszawskiego Instytutu Bankowości (WIB) oraz Związku Banków Polskich pn. „Postawy Polaków wobec cyberbezpieczeństwa 2024". Jednoznacznie wynika z niego, że coraz chętniej sięgamy po telefon korzystając z usług bankowych – tak zadeklarowała ponad połowa respondentów (57%). Logowanie do bankowości internetowej poprzez komputer deklaruje 30% badanych.

W JAKI SPOSÓB NAJCZĘŚCIEJ KORZYSTASZ Z USŁUG BANKOWYCH?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

2/ Z danych serwis cashless.pl: https://www.cashless.pl/15476-apple-pay-google-pay-liczba-platnosci-1-kw-2024

3/ Raport Fundacji Polska Bezgotówkowa i Spotdata pt. „Przyszłość płatności. W stronę bezpiecznego cyfrowego świata", listopad 2023 r.

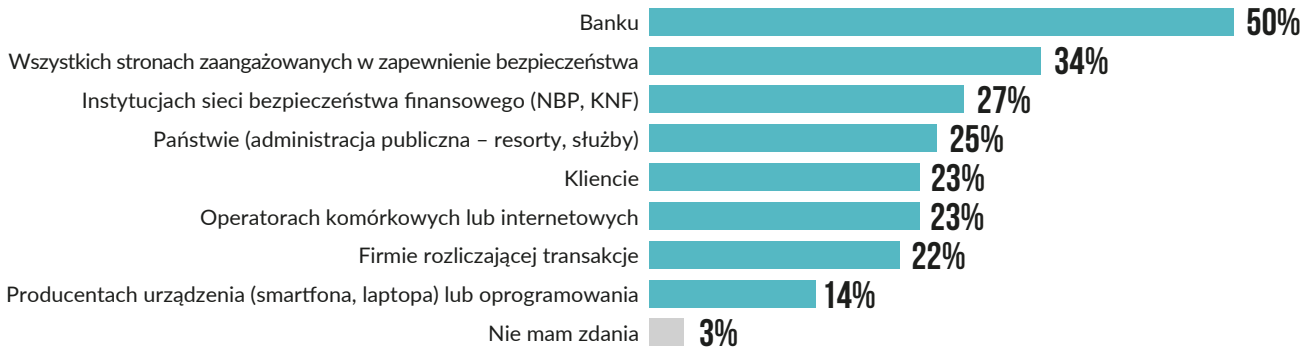
Według danych ZBP w I kwartale 2024 r. zainstalowano już 22,3 mln aktywnych aplikacji mobilnych i ta liczba stale rośnie[4]. Zwolenników płatności mobilnych widzimy szczególnie w grupie młodych dorosłych, ceniących sobie wygodę i nowoczesne technologie: 77% wśród 25–34-latków i 74% wśród 18-24-latków używa bankowości mobilnej na smartfonie lub tablecie. Niemniej jednak entuzjastów w tym zakresie odnajdziemy również wśród starszych Polaków w wieku 35–49 lat (68%) czy w grupie 50+ (39% z nich mobilnie korzysta z usług bankowych)[5].

BANKI NIEZMIENNIE LIDEREM CYBERBEZPIECZEŃSTWA

Wraz z rozwojem płatności elektronicznych (według danych Fundacji Polska Bezgotówkowa stanowią one obecnie około 65% wszystkich transakcji dokonywanych w Polsce[6]) kluczowym wyzwaniem stała się kwestia ich bezpieczeństwa. Z punktu widzenia sektora finansowego niezwykle istotne jest, aby za dużymi nakładami na infrastrukturę i ekspertów od cyberbezpieczeństwa w bankach podążali rzetelnie wyedukowani i świadomi użytkownicy usług elektronicznych.

Tymczasem, Polacy niezmiennie w większości uważają, że **odpowiedzialność za bezpieczeństwo finansowych usług cyfrowych spoczywa w dużej mierze na bankach**[7]. Podział tej odpowiedzialności pomiędzy kilkoma stronami dostrzega co trzeci z badanych. Istotna część Polaków uważa, że to instytucje bezpieczeństwa finansowego i administracja państwowa spełniają tutaj kluczową rolę. 23% badanych uważa, że jest ona po stronie operatorów komórkowych bądź internetowych, a 14% że na producentach urządzeń (typu smartfon, laptop) i oprogramowania.

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO USŁUG, W TYM TRANSAKCJI FINANSOWYCH DOKONYWANYCH W FORMIE ELEKTRONICZNEJ TWOIM ZDANIEM SPOCZYWA NA:



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

4/ Raport ZBP „Netbank. Bankowość internetowa i mobilna, płatności bezgotówkowe", dane za I kwartał 2024 r. (dla porównania w IV kwartale 2023 r. – było 21,7 mln aktywnych aplikacji mobilnych).

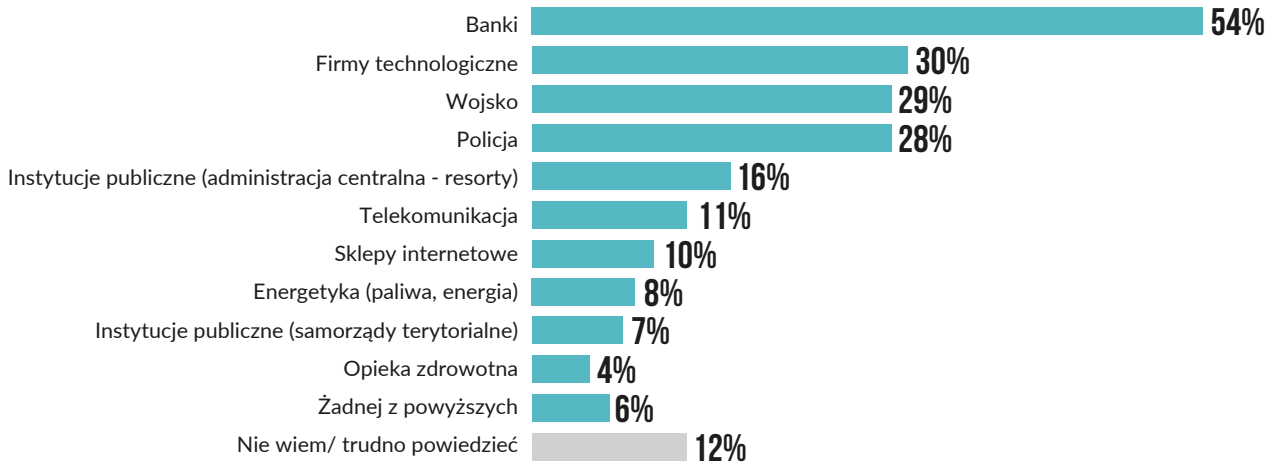
5/ Badanie WIB i ZBP „Postawy Polaków wobec cyberbezpieczeństwa 2024."

6/ Raport Fundacji Polska Bezgotówkowa i Spotdata pt. „Przyszłość płatności. W stronę bezpiecznego cyfrowego świata", listopad 2023 r.

7/ W porównaniu do wyników badania „Postawy Polaków wobec cyberbezpieczeństwa" z lat poprzednich

Wysoki wskaźnik odpowiedzialności banków za bezpieczeństwo naszych finansów koreluje z wysokim poziomem zaufania społecznego – banki od lat są niezmiennie uważane za liderów cyberbezpieczeństwa w Polsce. W czołówce zestawienia znalazły się również firmy technologiczne) i służby mundurowe.

KTÓRĄ Z PONIŻSZYCH BRANŻ LUB INSTYTUCJI POSTRZEGASZ JAKO LIDERÓW W ZAKRESIE CYBERBEZPIECZEŃSTWA?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

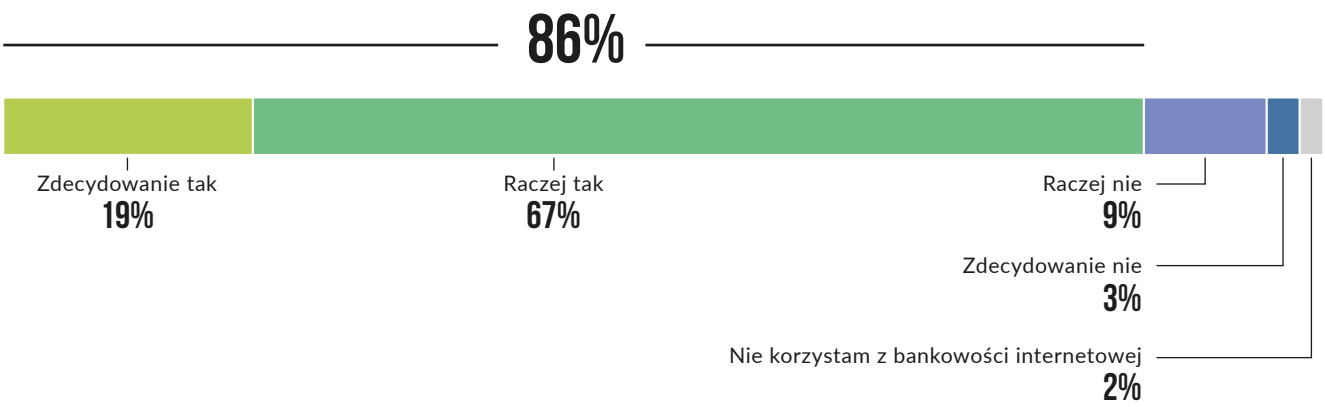
WYSOKI POZIOM BANKOWYCH ZABEZPIECZEŃ WPŁYWA NA POCZUCIE BEZPIECZEŃSTWA KLIENTÓW

Banki, aby jak najlepiej chronić swoich klientów, stosują zaawansowane zabezpieczenia, jak np.:

- WIELOPOZIOMOWĄ WERYFIKACJĘ TOŻSAMOŚCI
- SZYFROWANIE DANYCH PRZESYŁANYCH MIĘDZY KLIENTEM A BANKIEM
- SYSTEMY MONITOROWANIA I WYKRYWANIA PODEJRZANYCH TRANSAKCJI
- REGULARNE AUDYTY ZABEZPIECZEŃ I AKTUALIZACJA OPROGRAMOWANIA

Odpowiedzialne podejście banków, które stale dostosowują poziom zabezpieczeń do nowych cyberzagrożeń sprawia, że ich klienci, pomimo licznych zagrożeń zewnętrznych tak chętnie poruszają się po świecie bankowości elektronicznej. **Większość Polaków (86%) czuje się bezpiecznie korzystając z bankowości internetowej lub mobilnej**. Zdecydowane bezpieczeństwo odczuwają bardziej mężczyźni (24%) niż kobiety (15%). Najbardziej pewni swojego bezpieczeństwa są młodzi dorośli w wieku 18–24 lata – prawie co trzeci z nich nie ma co do tego żadnych wątpliwości. Co warto podkreślić, również 72% dojrzałych respondentów w wieku 50+ deklaruje, że raczej nie odczuwa zagrożenia korzystając z bankowości internetowej i mobilnej.

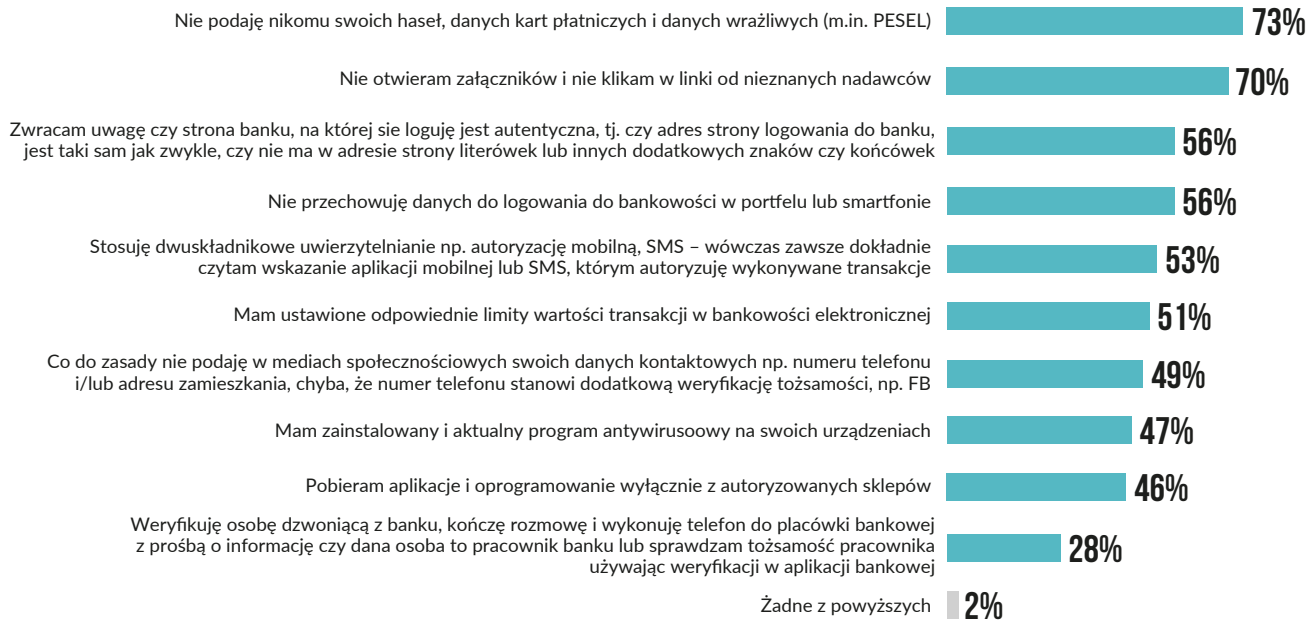
CZY CZUJESZ SIĘ BEZPIECZNIE KORZYSTAJĄC Z BANKOWOŚCI INTERNETOWEJ I MOBILNEJ?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

Wysokie poczucie bezpieczeństwa wynika nie tylko z zaangażowania samych banków, ale także poprawiającemu się (choć niekiedy w bólach) poziomowi świadomości i kompetencji cyfrowych klientów. Jak wynika z danych WIB „złotą zasadę" braku podawania haseł do bankowości, danych kart płatniczych ani innych danych wrażliwych stosuje już zdecydowana większość Polaków korzystających z elektronicznej bankowości (73%). Ponadto, 7 na 10 osób deklaruje, że nie otwiera załączników i nie klika w linki od nieznanych nadawców, a blisko 6 na 10 osób zwraca uwagę na autentyczność strony banku podczas logowania oraz nie przechowuje danych logowania do bankowości w portfelu lub smartfonie (56%). Nieco ponad połowa badanych stosuje dwuskładnikowe uwierzytelnianie (53%) lub ma ustawione limity transakcji w bankowości elektronicznej (51%).

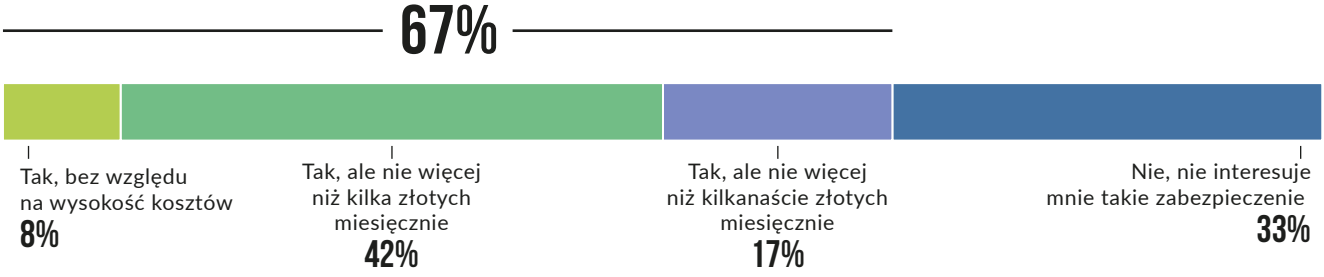
ZAZNACZ DO KTÓRYCH ZALECEŃ BANKOWYCH SIĘ STOSUJESZ:



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024”, badanie SW Research dla WIB

Pomimo, że Polacy czują się względnie swobodnie w przestrzeni cyfrowych finansów, to są skłonni ponosić dodatkowe opłaty za rozwiązania podnoszące poziom zabezpieczeń w bankowości elektronicznej – taką gotowość wyraziło 67% badanych. Jednak w większości akceptowalne jest przeznaczenie na ten cel tylko drobnych kwot w skali miesiąca – 42% respondentów chce inwestować w bezpieczeństwo internetowego konta bankowego lub bankowej aplikacji mobilnej nie więcej niż kilka złotych miesięcznie, a tylko 8% bez względu na wysokość kosztów.

CZY JESTEŚ SKŁONNY/A DO PONOSZENIA DODATKOWYCH, STAŁYCH MIESIĘCZNYCH KOSZTÓW PODNOSZĄCYCH POZIOM BEZPIECZEŃSTWA TWOICH E-FINANSÓW, W TYM NP. INTERNETOWEGO KONTA BANKOWEGO LUB BANKOWEJ APLIKACJI MOBILNEJ?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024”, badanie SW Research dla WIB

Osoby, które deklarowały chęć ponoszenia dodatkowych kosztów na poziomie kilku złotych miesięcznie to głównie osoby starsze 50+ (44%) – dla porównania zainteresowanie w tej kwestii młodych dorosłych w wieku 18–24 lat było na poziomie 34%. Chętniej o bezpieczeństwo e-finansów zadbałyby kobiety (45%) niż mężczyźni (39%).

„Nie jest zaskoczeniem, że Polacy oczekują głównie od banków dbałości o bezpieczeństwo powierzonych informacji i środków finansowych. To duża, ale też oczywista odpowiedzialność, jaka spoczywa na całym sektorze bankowym. Również nie dziwi opinia badanych, że banki są postrzegane jako liderzy cyberbezpieczeństwa – od wielu lat sektor finansowy rozwija swoje systemy bezpieczeństwa, stosuje najlepsze praktyki, aby w najwyższym stopniu utrudnić działania cyberprzestępców. Trzeba jednak zauważyć, że odpowiedzialność za bezpieczeństwo w przestrzeni cyfrowej spoczywa na nas wszystkich – bardzo ważnym ogniwem cyberbezpieczeństwa są ludzie. Cyberprzestępcy stosują metody manipulacji, które mają złamać czujność użytkowników systemów transakcyjnych. Dlatego banki oraz inne instytucje przykładają ogromną wagę do tzw. cyberedukacji, której celem jest podnoszenie świadomości o funkcjonujących cyberzagrożeniach. Ma to kolosalne znaczenie, ponieważ nawet najlepsze systemy bezpieczeństwa nie ochronią nas, jeśli nie zachowamy czujności i będziemy udostępniać swoje dane finansowe, loginy i hasła czy instalować niepożądane aplikacje”

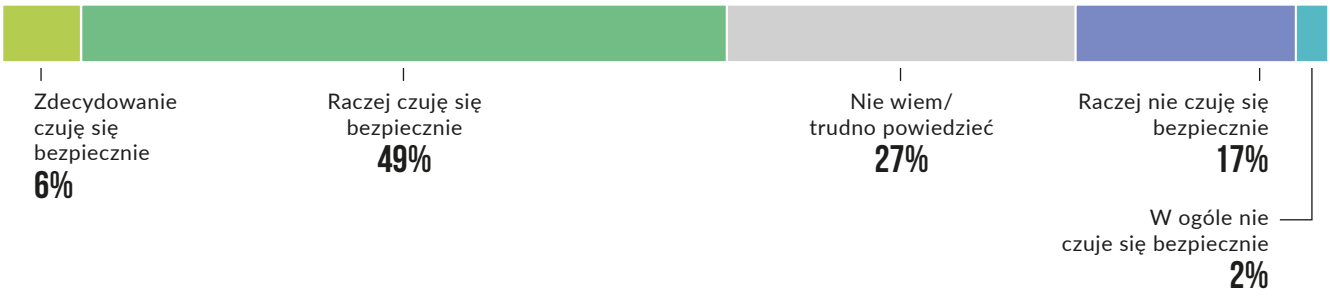
MICHAŁ MAZUR,
EKSPERT DS. CYBERBEZPIECZEŃSTWA,
DEPARTAMENT WYKRYWANIA CYBERZAGROŻEŃ
I FRAUDÓW TRANSAKCYJNYCH,
SANTANDER BANK POLSKA

ROZDZIAŁ III

Cyfrowy Świat: zagrożenia i zabezpieczenia

23,1 mln Polaków loguje się do bankowości internetowej co najmniej raz w miesiącu – tak wynika z danych Związku Banku Polskiego8/. Polacy przyzwyczaili się do bankowości online i czują się w niej dość pewnie. Jednak jej użytkownicy mają świadomość nie tylko korzyści, ale też zagrożeń, które kryją się za technologiami ułatwiającymi życie. Według badania WIB „Postawy Polaków wobec cyberbezpieczeństwa 2024" blisko co piąta badana osoba (17%) nie czuje się bezpiecznie w cyfrowym świecie korzystając z Internetu, Social Mediów czy komunikatorów. Natomiast prawie połowa – 49% deklaruje, że raczej poczucie bezpieczeństwa jest w ich przypadku na dość wysokim poziomie. W przestrzeni cyfrowej bardziej bezpiecznie czują się panowie (53%) niż panie (45%).

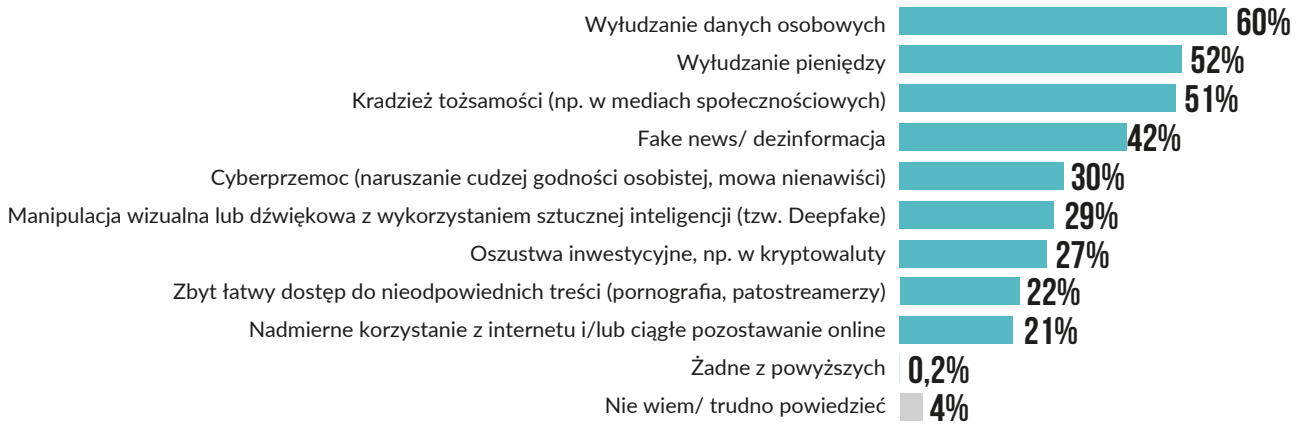
NA ILE BEZPIECZNIE CZUJESZ SIĘ W ŚWIECIE CYFROWYM, TJ. INTERNET, SOCIAL MEDIA, KOMUNIKATORY ITP.?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

Bez względu na własne poczucie bezpieczeństwa Polacy potrafią określić, co ich zdaniem stanowi największe zagrożenia w przestrzeni cyfrowej.

WSKAŻ OBSZARY, KTÓRE UWAŻASZ OBECNIE ZA NAJWIĘKSZE ZAGROŻENIA W PRZESTRZENI CYFROWEJ?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

8/ Raport ZBP „Netbank. Bankowość internetowa i mobilna, płatności bezgotówkowe", dane za I kwartał 2024 r.

Jak pokazuje badanie WIB, to tzw. phishing uważany jest przez Polaków za największe zagrożenie w przestrzeni cyfrowej. Respondenci najbardziej obawiają się, że w wyniku tego oszustwa zostaną wyłudzone ich dane (60% wykazało taką obawę) i pieniądze (52%).

O bezpieczeństwo danych osobowych martwią się bardziej osoby starsze w wieku 50+ (63% z nich określa kradzież danych największym zagrożeniem w sieci), a najmniej młodzi dorośli w wieku 18–24 lata (50%). Natomiast prawie co trzeci 18–24-latek zwraca uwagę na problem cyberprzemocy w przestrzeni cyfrowej (38%). Co ciekawe młodzi dorośli w porównaniu z osobami starszymi mniej obawiają się o przejęcie tożsamości w mediach społecznościowych, tj. 43% wśród 18–24-latków widzi w tym zagrożenie, natomiast większą obawę o taki rodzaj przestępstwa wyrażają osoby w wieku 35–49 lat (53%) i powyżej 50 lat (52%).

Obawy polskiego społeczeństwa dotyczące phishingu są uzasadnione. Jak wskazuje CERT Polska najpopularniejszym typem oszustw w sieci zarejestrowanych w całym 2023 r. były właśnie strony phishingowe. Cyberprzestępcy poprzez fałszywe strony wybranego banku, ale łudząco podobne do tych oryginalnych (np. różniące się jedną literą lub dodaniem innej frazy do adresu www) wyłudzają loginy i hasła do bankowości. W 2023 roku zarejestrowano 41 423 tego typu incydenty, co stanowi aż 52% wszystkich obsłużonych incydentów przez CERT – to wzrost o ponad 61 pkt. proc. w porównaniu do 2022 roku[9].

CERT[10] wskazuje, że najpopularniejszymi kampaniami phishingowymi były te, które podszywały się pod popularne serwisy, takie jak:

aukcyjne Allegro – **11 161 przypadków**	społecznościowy Facebook – **5 308 przypadków**	sprzedażowy OLX – **4 753 przypadki**[11]

Serwis Allegro wraz z rozwojem swojej funkcjonalności tworzył odpowiednie struktury bezpieczeństwa - traktujemy je jako jedno z naszych zobowiązań wobec klientek i klientów. Aktualnie pracuje u nas szereg zespołów, których zadaniem jest poprawa bezpieczeństwa naszych użytkowniczek i użytkowników. W ramach tych zespołów ponad 100 osób stale obserwuje trendy w cyberbezpieczeństwie, stara się reagować w przypadku wykrycia jakichkolwiek prób cyberataku i zgłaszać je odpowiednim organom - w tym CERT Polska, do którego w samym 2023 roku wysłaliśmy blisko 7 tysięcy zgłoszeń fałszywych domen podszywających się pod nasz serwis. Ponadto, wspólnie z Warszawskim Instytutem Bankowości oraz Wydziałami Prewencji Policji, prowadzimy szereg działań edukacyjnych mających na celu podnoszenie świadomości bezpieczeństwa polskich Internautów i ich wiedzy o bezpieczeństwie w przestrzeni cyfrowej, tak aby w obliczu potencjalnego ataku phishingowego nasi odbiorcy nie tylko odpowiednio go wychwycili, ale również na niego nie reagowali oraz zgłaszali nam fakt zaistnienia takiego zagrożenia.

MARIUSZ TOKARSKI,
KIEROWNIK ZESPOŁU DS. WSPÓŁPRACY Z ORGANAMI ŚCIGANIA, **ALLEGRO**

9/ Źródło danych – NASK: „Raport roczny z działalności CERT Polska 2023", publikacja z dn. 17.04.2024 r.
10/ Skrót CERT to z ang. Computer Emergency Response Team, tj. Zespół reagowania na incydenty komputerowe – źródło NASK
11/ Źródło danych - NASK: „Raport roczny z działalności CERT Polska 2023", publikacja z dn. 17.04.2024 r.

Do styczności z oszustwami dokonywanymi elektronicznie (takimi jak phishing czy malware), osobiście lub w swoim otoczeniu, przyznaje się 62% badanych Polaków.

CZY SPOTKAŁEŚ/AŚ SIĘ (OSOBIŚCIE LUB W TWOIM OTOCZENIU) Z NASTĘPUJĄCYMI OSZUSTWAMI DOKONYWANYMI ELEKTRONICZNIE?

Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

MALWARE to kradzież danych poprzez nieświadomą instalację złośliwego oprogramowania, takiego jak trojany i inne wirusy.

PHISHING to oszustwo, którego nazwa nie bez kozery powiązana jest z ang. słowem „fishing", czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze stosują przynętę, tj. podszywają się np. pod osobę zaufania publicznego lub instytucję/firmę za pośrednictwem fałszywych e-maili, stron www czy SMS-ów, aby zdobyć poufne informacje (takie jak login i hasło do banku, PESEL) w celu kradzieży pieniędzy – coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych, np. poprzez „metodę na BLIK-a".

Warto również pamiętać, że **phishing może mieć różne oblicza**, tj. może być stosowany nie tylko w formie online – **jednym z nich jest tzw. vishing** (z ang. voice phishing), **tj. oszustwo przez telefon**. Dopuszczając się go przestępcy dzwonią z nieznanych numerów i podszywają się zazwyczaj pod osobę zaufania publicznego (np. policjanta, lekarza, pracownika ZUS) w celu wyłudzenia danych lub pieniędzy. Dotyczy to również połączeń telefonicznych od rzekomych przedstawicieli banków. Niestety tylko 28% Polaków weryfikuje osobę dzwoniącą z banku w ten sposób, że kończy rozmowę i wykonuje telefon do placówki bankowej z prośbą o potwierdzenie danego pracownika lub samemu sprawdza tożsamość dzwoniącej osoby, używając weryfikacji w aplikacji bankowej[12].

DEZINFORMACJA – WYZWANIEM „TU I TERAZ"

Innym, wymagającym działań prewencyjnych zjawiskiem, jest problem dezinformacji, który może skutecznie zakłócać funkcjonowanie społeczeństw. W dobie sztucznej inteligencji umożliwiającej tworzenie coraz bardziej zaawansowanych i trudnych do wykrycia fałszywych treści, zagrożenie to staje się jeszcze bardziej niebezpieczne. Potwierdzają to **wyniki badania WIB, w którym 42% respondentów wskazało właśnie dezinformację i fake newsy jako czwarte największe zagrożenie we współczesnym cyfrowym świecie**.

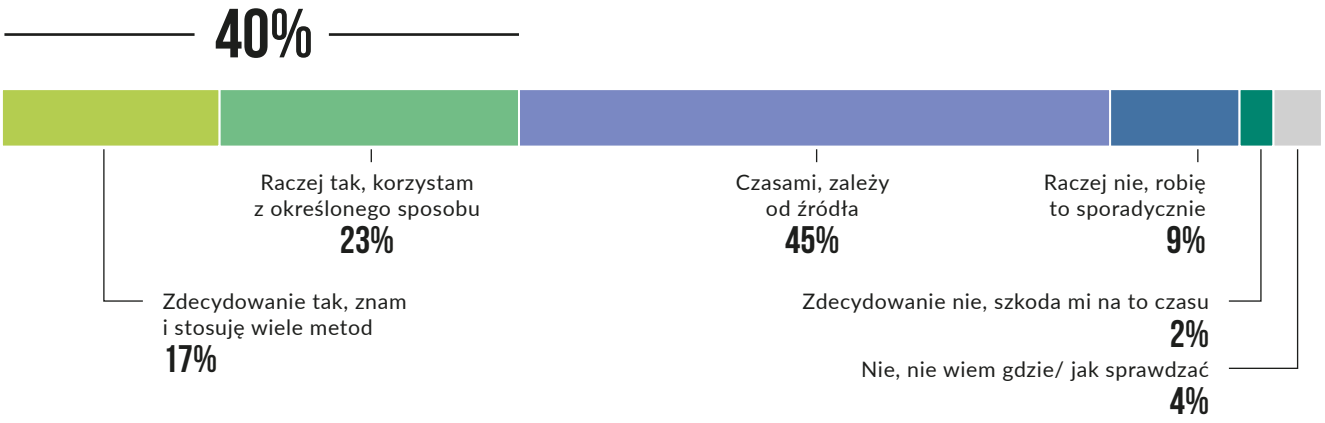
Problem dezinformacji wydaje się przybierać na sile w ostatnich latach – z tegorocznego badania Koalicji Razem Przeciw Dezinformacji pt. „Dezinformacja oczami Polaków" wynika, że aż 81% badanych jest zdania, że w ciągu ostatniej dekady wzrosła skala rozpowszechnianej w Internecie

12/ Dane z wykresu badania WIB „Postawy Polaków wobec cyberbezpieczeństwa 2024" – str. 13 tego raportu

dezinformacji. Może mieć ona negatywny wpływ na gospodarkę, politykę, a nawet nastroje czy zdrowie publiczne – stąd tak ważne jest, aby m.in. potwierdzać prawdziwość informacji w kilku źródłach.

Dane WIB pokazują, że 40% Polaków sprawdza wiarygodność informacji przeczytanych w Internecie, ale tylko część z nich (17%) stosuje w tym celu wiele metod, a 23% korzysta z jednego określonego sposobu. Z kolei 45% weryfikuje informacje tylko czasami – w zależności od źródła, w jakim odnaleźli daną informację.

CZY W JAKIKOLWIEK SPOSÓB SPRAWDZASZ WIARYGODNOŚĆ INFORMACJI, KTÓRE PRZECZYTAŁEŚ/AŚ W INTERNECIE?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024”, badanie SW Research dla WIB; możliwość wyboru wielu odpowiedzi

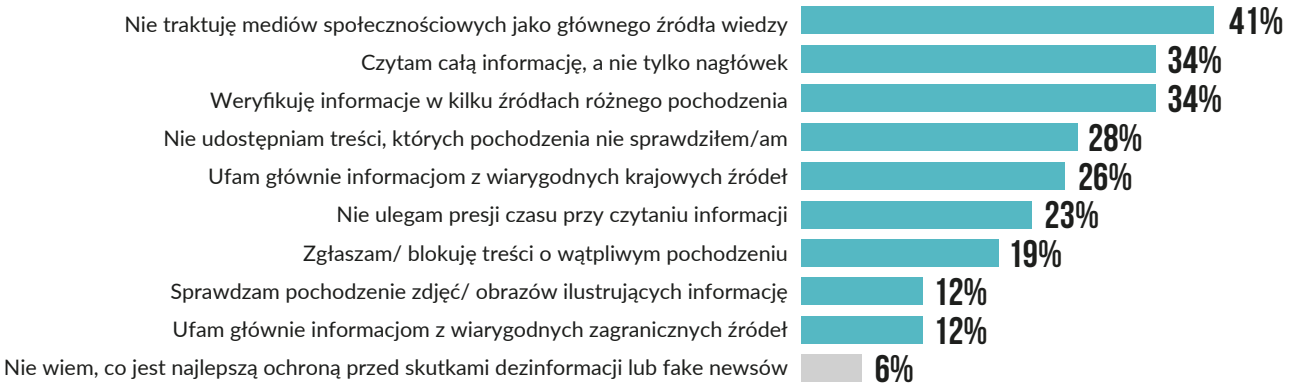
Polacy stosują różne strategie, aby chronić się przed dezinformacją lub wpływem fake newsów. Najbardziej popularną metodą jest nietraktowanie mediów społecznościowych jako głównego źródła wiedzy – ten sposób wskazało 41% respondentów badania „Postawy Polaków wobec cyberbezpieczeństwa 2024”.

Niestety zdecydowanie rzadziej korzystamy z tych najbardziej skutecznych metod ochrony – tylko co trzecia osoba czyta całą informację, a nie tylko nagłówek (tj. ochrona przed tzw. clikbaitami) oraz weryfikuje informacje w kilku źródłach różnego pochodzenia (34%).

Innymi popularnymi wśród ankietowanych sposobami ograniczania negatywnego wpływu dezinformacji i fake newsów są: nieudostępnianie treści, których pochodzenia się nie sprawdziło wcześniej (28%), nieuleganie presji czasu podczas czytania informacji (23%) oraz zgłaszanie lub blokowanie treści o wątpliwym pochodzeniu (19%).

Warto również zauważyć, że Polacy ufają bardziej krajowym źródłom informacji (26%) niż tym zagranicznym (12% ma zaufanie do wiarygodnych mediów z zagranicy).

JAKIE SPOSOBY SĄ TWOIM ZDANIEM NAJLEPSZĄ OCHRONĄ PRZED SKUTKAMI DEZINFORMACJI LUB FAKE NEWSÓW? PROSZĘ WYBRAĆ MAKS. 3 ODPOWIEDZI.

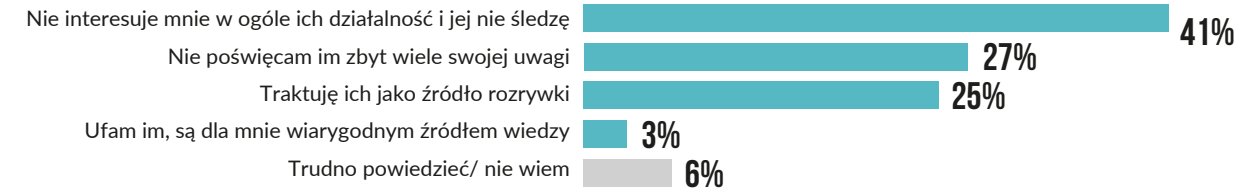


Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

Badanie wykazało, że część Polaków nie traktuje mediów społecznościowych jako głównego źródła informacji, ale też nie ufa treściom w nich zamieszczanym. Jedynie 11% badanych ufa treściom z Facebooka, zaledwie 6% – z portalu X (dawn. Twitter) i Instagrama, a 5% tym pochodzącym z TikToka czy LinkedIna.

Krytyczny stosunek do platform społecznościowych powinien uwzględniać również wyważone podejście do działalności tzw. influencerów. Według danych WIB 41% ankietowanych w ogóle nie jest zainteresowanych ich działalnością i jej nie śledzi, a 27% nie poświęca ich działalności zbyt wiele uwagi. Z kolei jedna czwarta badanych (25%) traktuje influencerów jako źródło rozrywki. Tylko niewielki odsetek badanych (3%) ufa im i uważa ich za wiarygodne źródło wiedzy.

JAKI MASZ STOSUNEK DO DZIAŁALNOŚCI INFLUENCERÓW W SIECI?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

Skoro Polacy wykazują niskie zaufanie do influencerów i mediów społecznościowych, nasuwa się pytanie: komu ufają w sieci? TOP3 zaufanych źródeł internetowych według Polaków: strony administracji państwowej (44%), wyniki w wyszukiwarce Google (34%) oraz portale internetowe mediów tradycyjnych (np. gazet czy agencji prasowych) (24%).

TREŚCIOM, Z KTÓRYCH ŹRÓDEŁ INTERNETOWYCH UFASZ NAJBARDZIEJ? WSKAŻ MAX. 3 ŹRÓDŁA.

Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

„Jak wynika z badań WIB, Polacy starają się radzić sobie z negatywnym zjawiskiem dezinformacji głównie poprzez dywersyfikowanie źródeł informacji i nieopieranie się na wiadomościach publikowanych w mediach społecznościowych. Jednak ilość czasu spędzanego online wciąż rośnie, zwłaszcza wśród młodych ludzi. Badanie NASK Nastolatki 3.0 pokazuje, że grupa ta korzysta z Internetu średnio 5 godz. i 36 min dziennie. Im dłuższy kontakt z informacjami mamy, tym łatwiej bezrefleksyjnie przyswajamy ich treść. Dlatego oprócz ograniczenia dopływu informacji, powinniśmy także wzmacniać kompetencję krytycznego myślenia.
Pomocny może być w tym schemat 4Z, tj. weryfikujmy:

- → czy źródło informacji jest wiarygodne – sprawdźmy czy można zaufać osobie, czy portalowi, który podał informację;
- → rzetelność i logikę przedstawionej sytuacji – zastanówmy się, czy opisana sytuacja ma sens, a wydarzenia brzmią prawdopodobnie;
- → czy tę samą informację potwierdza inne źródło;
- → co jest opinią autora, a co faktem – weryfikując treści, pamiętajmy, że należy odróżniać fakty od opinii, by móc samodzielnie wyciągać wnioski i formułować własne zdanie.

→

Rozwijanie umiejętności krytycznego myślenia należy uczyć już od najmłodszych lat, stąd NASK we współpracy z międzynarodowymi partnerami prowadzi projekt Make It Clear, którego celem jest budowanie odporności młodzieży na dezinformację i wyposażenie edukatorów w narzędzia do edukacji w tym obszarze”

KAMIL OLESZKIEWICZ,
DZIAŁ PROFILAKTYKI CYBERZAGROŻEŃ
NASK-PIB.

NAJSŁABSZYM OGNIWEM W SIECI BEZPIECZEŃSTWA NIESTETY NA OGÓŁ JEST CZŁOWIEK

Jak już wspomniano, w cyfrowym świecie można obecnie napotkać wiele zagrożeń: od wyłudzania pieniędzy i danych osobowych (tj. phishing), po kradzieże tożsamości w social mediach, oszustwa inwestycyjne, aż do dezinformacji i cyberprzemocy.

Z danych WIB wynika, że staramy się dbać o bezpieczeństwo w przestrzeni cyfrowej, ale głównie przy okazji korzystania z bankowości elektronicznej, a także w zakresie stosowania zabezpieczeń przed atakami typu malware, czyli chronimy się przede wszystkim przed wirusami. W przeważającej większości używamy oprogramowania antywirusowego na komputerze lub laptopie (78% badanych zadeklarowało, że posiada aktualne zabezpieczenia). Zwiększa się również troska o bezpieczeństwo naszych smartfonów: o 7 pkt. proc. wzrosło instalowanie oprogramowania antywirusowego na telefonie komórkowym (z 52% w 2023 r. do 59% w 2024 r.). Niestety ciągle nie mamy wystarczającej świadomości, że smartfon też trzeba zabezpieczać przed wirusami – 17% badanych nie ma w ogóle wiedzy czy dysponuje antywirusem w swoim telefonie[13].

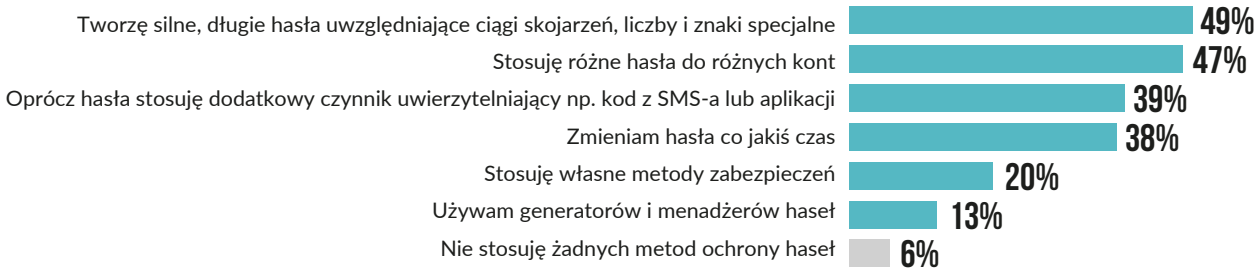
13/ W porównaniu do badania WIB i ZBP „Postawy Polaków wobec cyberbezpieczeństwa 2023.”

„Można w pewnym sensie przyznać, że faktycznie trudniej skutecznie zaatakować telefon komórkowy niż komputer osobisty pracujący na systemie Windows. Wynika to z różnic w działaniu systemów operacyjnych na tych urządzeniach. Niestety, jeśli wyciągamy z tego wniosek, że telefonu nie musimy chronić, jest to już zbyt daleko idące uproszczenie. Jeśli rezygnujemy z ochrony smartfona to wystawiamy się na podwyższone ryzyko. Bardzo często, jednym z elementów przygotowania skutecznego ataku na nasze konto bankowe jest właśnie zainstalowanie złośliwego oprogramowania na telefonie. Taki złośliwy program może chociażby przejmować wysyłane na telefon hasła jednorazowe. Niestety złośliwe aplikacje możemy napotkać również w oficjalnych sklepach Google Play czy App Store, bo okazuje się, że ich właściciele coraz słabiej kontrolują udostępniane tam oprogramowanie. Dlatego korzystanie z programu zabezpieczającego na telefonie komórkowym należy uznać za niezbędny dla naszego bezpieczeństwa standard. Z drugiej strony – coraz więcej ataków, które mają na celu kradzież naszych pieniędzy bazuje na socjotechnice lub technikach zupełnie niezwiązanych z naszym urządzeniem. Cyberprzestępcy tworzą bardzo różne scenariusze, z wykorzystaniem podszywania się pod osoby trzecie czy zaufane numery telefonów banków (spoofing). Dlatego, nawet kiedy korzystamy z dobrej jakości programu zabezpieczającego musimy pamiętać, że żadne zabezpieczenie nie uchroni nas przed sytuacją, w której dajemy się oszukać i sami zlecamy przelew, z którego korzystają przestępcy. Na tego typu scenariuszach polegają popularne oszustwa tzw. „na Blika" i tym podobne – w takich sytuacjach ofiara sama zleca transfer pieniędzy, zwiedziona działaniem cyberoszustów."

PAWEŁ JUREK,
DYREKTOR ROZWOJU BIZNESU
W **DAGMA BEZPIECZEŃSTWO IT**

Ponadto wciąż zbyt mało Polaków przywiązuje uwagę do tworzenia bezpiecznych haseł dostępu w Internecie, np. do poczty, banku czy mediów społecznościowych. Tylko 49% respondentów deklaruje, że tworzy zalecane silne hasła, tj. długie zawierające skojarzenia, liczby i znaki specjalne, 47% stosuje różne hasła do różnych kont, a 38% zmienia hasła co jakiś czas. Niestety tylko 39% używa dwuskładnikowego uwierzytelniania, np. kodu z SMS-a lub aplikacji. Mało z nas korzysta również z generatorów i menadżerów haseł – 13%.

CO ROBISZ, ŻEBY ZABEZPIECZAĆ SWOJE HASŁA (NP. DO POCZTY E-MAIL, BANKU, MEDIÓW SPOŁECZNOŚCIOWYCH)?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

PONIŻEJ ZESTAWIENIE NAJPOPULARNIEJSZYCH HASEŁ UŻYWANYCH PRZEZ POLAKÓW, WSKAZANYCH PRZEZ CERT POLSKA – NIESTETY CIĄGLE NAJCHĘTNIEJ WYBIERANE SĄ TE MAŁO BEZPIECZNE[14]:

123456	monika	123123	maciek	myszka	madzia	haslo1	dupa123	komputer1	qwerty12
qwerty	marcin	0	samsung	11111	dupa	abc123	kochamcie	klaudia	tomek1
12345	mateusz	bartek	qwertyuiop	1qazxsw2	morele	matrix	123321	pakistan	123456a
123456789	agnieszka	damian	zxcvbnm	lukasz	misiaczek	dragon	aaaaaa	magda	kamila
zaq12wsx	123qwe	michal	kasia	mateusz1	1q2w3e	wojtek	kamil1	wiktoria	magdalena
1234	1234567890	qwe123	1q2w3e4r	komputer	1111	marcin1	monika1	agnieszka1	michal1
12345678	1qaz2wsx	polska1	kochanie	666666	dupadupa	niunia	kamil	mariusz	lolek123
polska	1234567	password	lol123	qazwsx	weronika	haslo	patryk	barcelona	654321
111111	qwerty123	karolina	kasia1	piotrek	master	kosama	sebastian	bartek1	zaq1@WSX

W przypadku używania ww. prostych ciągów znaków, potencjalnemu hakerowi złamanie hasła zajmie mniej niż sekundę! Stąd tak ważne jest, aby używać trudnych haseł – obecnie zalecana metoda to nawet 15 znaków i więcej (większość programów do łamania haseł testuje ciągi do 12 znaków)[15].

14/ Źródło: https://cert.pl/hasla/
15/ Źródło CERT Orange: https://cert.orange.pl/warto-wiedziec/bezpieczne-hasla/

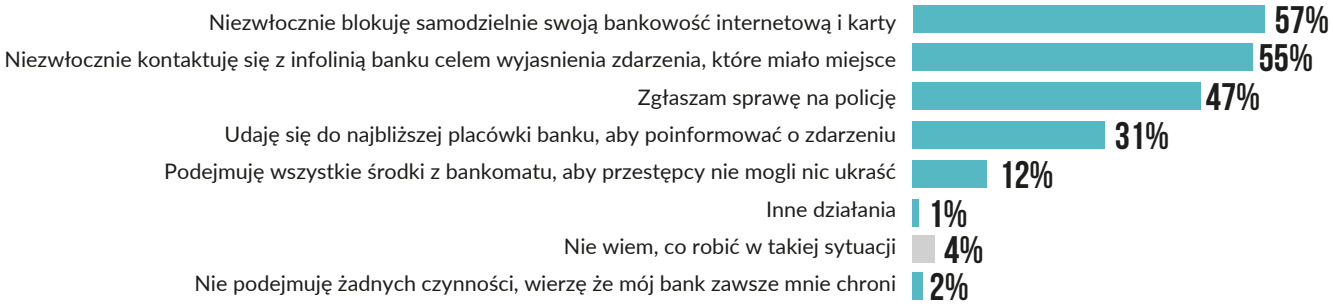
„Nie wszyscy użytkownicy Internetu zdają sobie sprawę z zagrożeń związanych z używaniem słabych haseł i brakiem dodatkowych zabezpieczeń, np. weryfikacji dwuetapowej. Kradzież danych, przejęcie skrzynki pocztowej lub profili w mediach społecznościowych, może prowadzić do utraty oszczędności lub wyłudzeń finansowych. Wielu z nas idzie na skróty, a tym samym wybiera proste i łatwe do zapamiętania hasła, w dodatku stosuje je w różnych usługach. Wśród wielu panuje błędne przekonanie, że weryfikacja dwuetapowa jest skomplikowana i czasochłonna, a obawa przed utratą urządzenia za pomocą którego otrzymują drugi składnik, budzi niechęć do tego typu rozwiązań. Warto wiedzieć, że silne hasła i uwierzytelnianie dwuskładnikowe to jedne z najprostszych, a jednocześnie najbardziej skutecznych rozwiązań, które chroni nas przed różnego typu zagrożeniami, zwłaszcza tymi, które mogą skutkować kradzieżą naszych danych i środków finansowych. W tworzeniu silnego hasła mogą pomóc generatory haseł, jednak ustawione w ten sposób hasło, może być trudne w zapamiętaniu. Lepszym rozwiązaniem są zatem menadżery haseł, które nie tylko przechowują nasze zaszyfrowane hasła, ale również mogą je generować. W celu ochrony naszych danych, a tym samym środków finansowych, warto poświęcić klika minut i zadbać o bezpieczeństwo naszych haseł oraz włączyć weryfikację dwuetapową”

ANNA KWAŚNIK, EKSPERTKA DS. BUDOWANIA WIADOMOŚCI CYBERBEZPIECZEŃSTWA, **NASK-PIB**

POSTĘPOWANIE W PRZYPADKU CYBEROSZUSTWA

Kiedy już cyberprzestępcy uda się złamać hasło lub w inny sposób „zhakować” zabezpieczenia naszego komputera czy telefonu - to czy wiemy, jak się zachować? Okazuje się, że w większości przypadków (choć niedostatecznie dużej) Polacy wiedzą, jak postąpić, kiedy podejrzewają, że padli ofiarą cyberprzestępców i ich konto bankowe jest zagrożone. Kluczowe są trzy główne kierunki, które zresztą wskazali respondenci: blokada konta (57%), kontakt z bankiem (55%) i zgłoszenie na policję (47%).

CO ROBISZ, JEŚLI PODEJRZEWASZ ŻE PADŁEŚ/AŚ OFIARĄ OSZUSTWA I TWOJE KONTO BANKOWE JEST ZAGROŻONE?



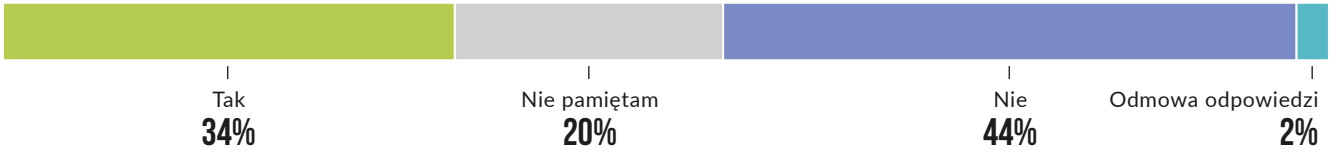
Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

„W sytuacji, gdy zdajemy sobie sprawę, że przestępca, w taki czy inny sposób, posiadł dane umożliwiające mu zalogowanie się do naszej bankowości internetowej – kluczowy jest czas. Należy jak najszybciej zablokować mu tę możliwość. Możemy to zrobić sami lub z pomocą specjalisty banku. Rekomendowane jest połączenie tych dwóch metod, a zatem jeśli potrafimy to najpierw samemu blokujemy bankowość elektroniczną i karty, po czym dzwonimy do banku powiadamiając o incydencie i prosimy specjalistę o sprawdzenie ustawień systemu. Specjalista, gdy będzie taka potrzeba, zaleci kolejne działania, w tym może to być również konieczność zgłoszenia sprawy Policji. Wynik badania pokazuje, że Polacy dobrze rozumieją konieczność działania w takiej sytuacji i w ankiecie wskazywali właściwe odpowiedzi. Pamiętajmy jednak, że w przypadku wielu przestępstw klient niestety nie ma świadomości, że padł ofiarą oszusta, a gdy się orientuje, bywa że jest już za późno. Dlatego tak ważne jest, aby klienci na bieżąco śledzili komunikaty bezpieczeństwa, które otrzymują od banków. Tam opisane są metody działań przestępców, którzy chcą wyłudzić od nas dane lub nakłonić nas do realizacji ich poleceń. Rozumienie tych mechanizmów i stosowanie dobrych praktyk wzmacnia nasze bezpieczeństwo w sieci."

TOMASZ CHMIELEWSKI,
GŁÓWNY EKSPERT W OBSZARZE BANKOWOŚCI ELEKTRONICZNEJ,
ING BANK ŚLĄSKI

Natomiast biorąc pod uwagę liczbę incydentów phishingowych zgłaszanych do CERT Polska, zadziwia że tylko 34% badanych przyznaje, że powiadamia o próbie tego rodzaju oszustwa – prawdopodobnie reszta takich przypadków nie jest w ogóle zgłaszana lub osoby nie są świadome, że były potencjalną ofiarą phishingu.

CZY KIEDYKOLWIEK ZGŁOSIŁAŚ/EŚ PRÓBĘ OSZUSTWA (NP. FAŁSZYWĄ STRONĘ, WIADOMOŚĆ, POŁĄCZENIE TELEFONICZNE)?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB

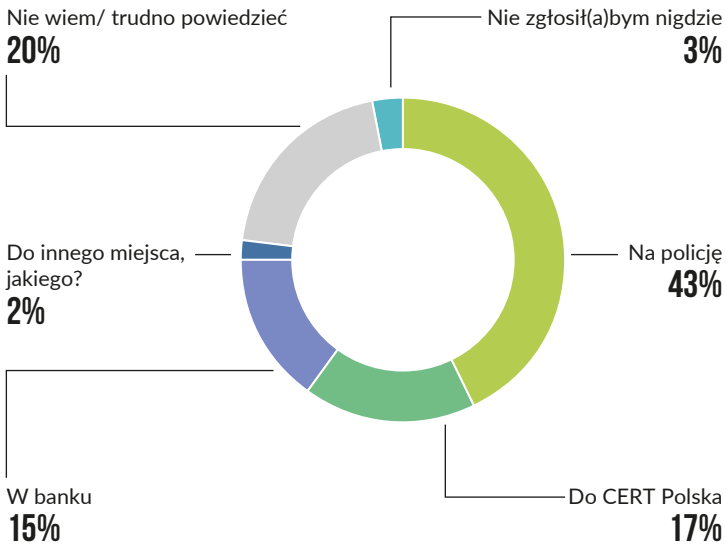
Ponad 4 osoby na 10 deklaruje, że powiadamia w pierwszej kolejności policję o próbie ataku phishingowego (43%), dopiero potem CERT Polska - 17%, a następnie bank (15%). Natomiast 2% badanych zgłasza próbę oszustwa do innych miejsc, np. do administracji strony, na której próbowano dokonać oszustwa. Warto zaznaczyć, że niestety co piąta osoba nie wie, gdzie zgłosiłaby działania cyberprzestępców.

WARTO WIEDZIEĆ, GDZIE ZGŁOSIĆ PRÓBY LUB ZAISTNIENIE PHISHINGU!

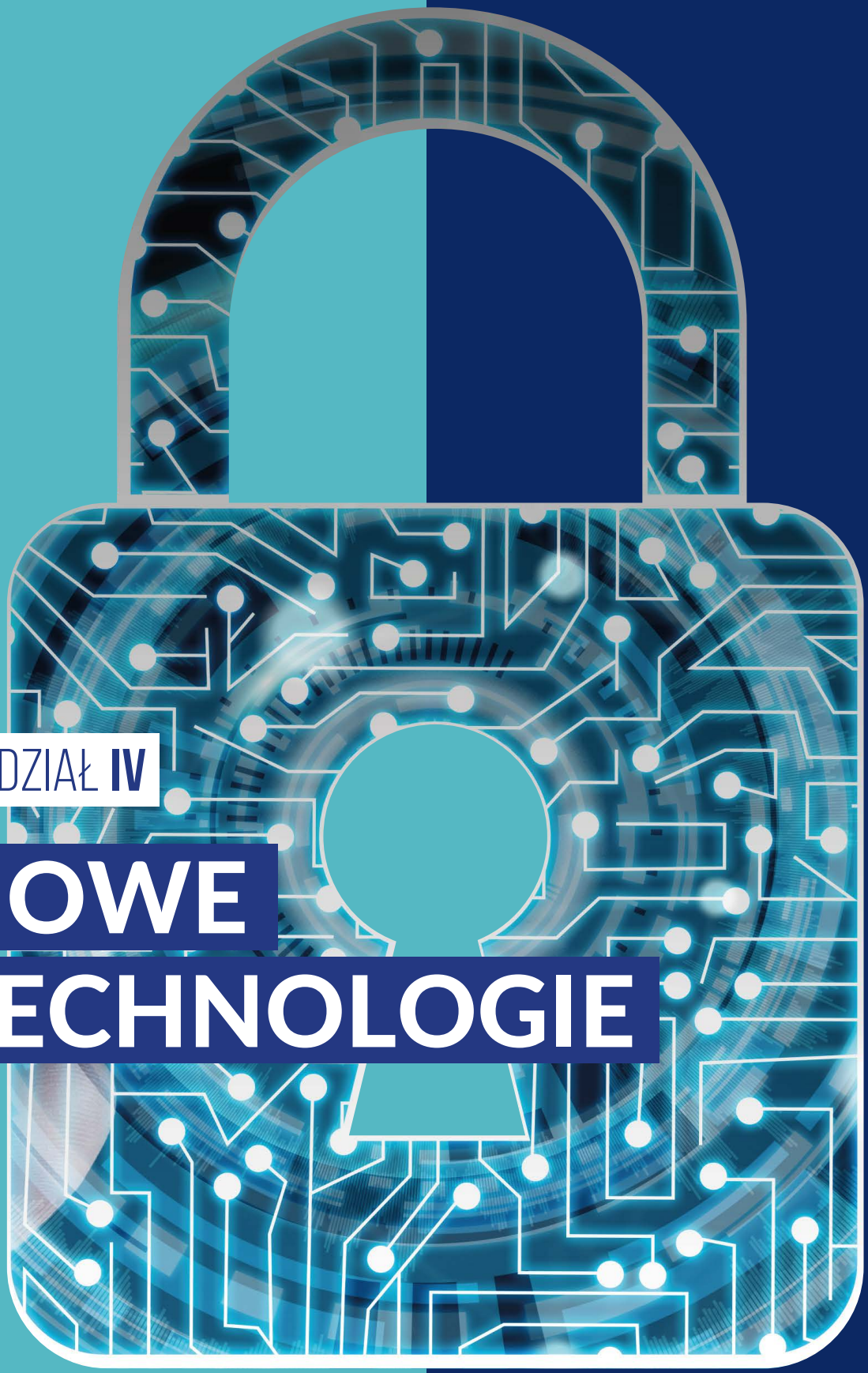
Do CERT Polska (tj. CSIRT NASK) na 2 sposoby:

- za pośrednictwem formularza na stronie https://incydent.cert.pl
- za pośrednictwem SMS-a na numer 8080 przekaż całą wiadomość dokumentującą phishing (nie wycinaj odnośnika ani treści) – wiadomość trafi bezpośrednio do analityków CERT Polska.

GDZIE ZGŁOSIŁBYŚ/ABYŚ PRÓBĘ OSZUSTWA (NP. FAŁSZYWĄ STRONĘ, WIADOMOŚĆ, POŁĄCZENIE TELEFONICZNE)?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB



ROZDZIAŁ **IV**

NOWE TECHNOLOGIE

Po pojawieniu się kart płatniczych wraz z postępem technologicznym na rynek weszły płatności mobilne, które zdobyły serca Polaków. Jednak patrząc w przyszłość może się okazać, że niebawem płatności mobilne będą ustępowały miejsca bardziej zaawansowanej formie autoryzacji płatności – biometrii.

Jak wynika z danych WIB transakcje w sklepach za pomocą danych biometrycznych stają się coraz bardziej pożądaną formą płatności – 43% badanych deklaruje chęć weryfikacji płatności odciskiem palca lub próbką głosu. Polacy przychylają się zatem do koncepcji wdrażania technologii przyśpieszających płatności, a uwierzytelnianie biometryczne może to ułatwić.

Dane wskazują, że chęć stosowania biometrii podczas zakupów deklarują osoby w różnym wieku – w przedziale wiekowym od 18 do 49 lat połowa badanych opowiedziała się za taką formą autoryzacji płatności. Natomiast w podziale na płeć mniej entuzjastycznie podchodzą do technologii biometrycznych kobiety niż mężczyźni: 38% kobiet i 49% mężczyzn wskazało chęć płacenia głosem lub odciskiem palca.

CZY CHCIAŁBYŚ/ABYŚ KORZYSTAĆ Z BIOMETRYCZNYCH METOD AUTORYZACJI PŁATNOŚCI, TAKICH JAK REALIZACJA TRANSAKCJI PO WERYFIKACJI PRÓBKI GŁOSU LUB ODCISKU PALCA?

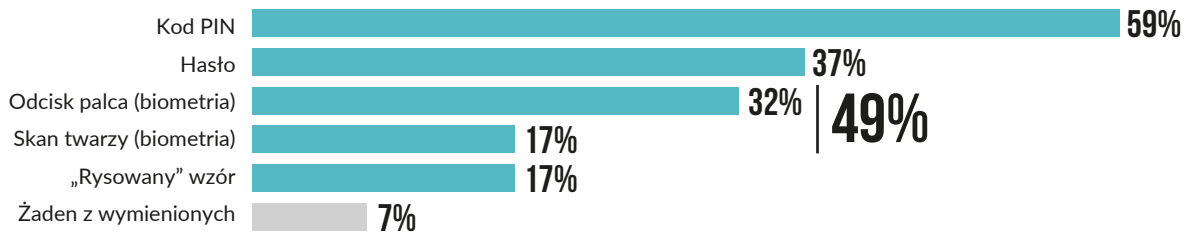
Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

„Biometria będzie jednym z trendów, który nada kształt przyszłości płatności. To bardzo użyteczne narzędzie, które nie tylko zapewnia bezpieczeństwo, ale także usprawnia proces zakupowy. Kontur twarzy, tęczówka oka czy odcisk palca są dużo bardziej unikatowym sposobem weryfikacji tożsamości niż wzór na ekranie, czy kod. Rozwój biometrii ma ogromny potencjał, a razem z rozwiązaniami takimi jak, cyfrowa tożsamość może uprościć nasze życie, a także chronić osoby prywatne, jak i przedsiębiorstwa. Polscy konsumenci są gotowi na biometryczne metody uwierzytelniania płatności, doceniając szybkość, wygodę i bezpieczeństwo tych rozwiązań. VISA chce być w czołówce zmian, które mają zapewnić klientom i sprzedawcom spokój ducha i pewność, że są lepiej chronieni w świecie cyfrowym. Dlatego w ciągu ostatnich 5 lat zainwestowaliśmy ponad 10 mld dolarów w technologię w celu zmniejszenia liczby oszustw i zwiększenia bezpieczeństwa sieci. Efekty tych działań są widoczne, odsetek oszustw w sieci Visa należy do najniższych we wszystkich formach płatności”

DIANA GONTAR,
DYREKTORKA DS. ZARZĄDZANIA RYZYKIEM
W REGIONIE EUROPY ŚRODKOWO-WSCHODNIEJ, **VISA**

Biometria stanowi również sposób zabezpieczenia telefonów. Choć najczęstszą blokadą jest nadal kod PIN – stosuje ją 59% badanych, to już prawie połowa Polaków (49%) zabezpiecza dostęp do swojego smartfonu za pomocą technologii biometrycznych, tj. odciskiem palca i skanem twarzy. Biometrię wolą stosować młodzi dorośli: 42% osób w wieku 18-24 lata odblokowuje telefon odciskiem palca, a 32% 25-34-latków skanem twarzy. Natomiast osoby starsze 50+ preferują blokadę hasłem - 45% stosuje takie zabezpieczenie.

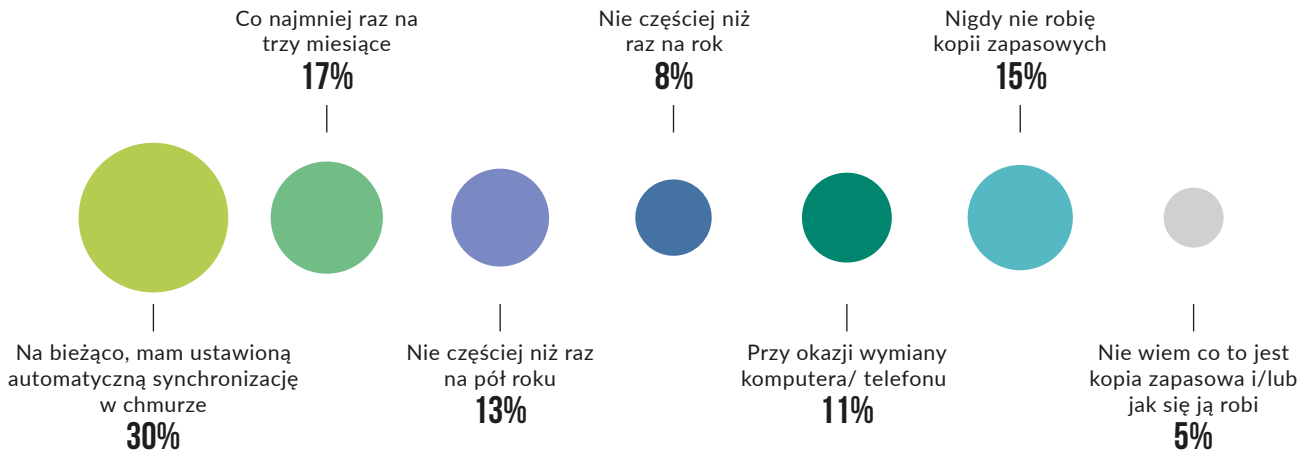
JAKI TYP ZABEZPIECZENIA BLOKADY/ DOSTĘPU DO EKRANU DO TELEFONU STOSUJESZ?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024”, badanie SW Research dla WIB.

Wykorzystanie technologii dla zabezpieczania swoich danych stosowane jest także w przypadku korzystania z chmury. Tworzenie w niej kopii zapasowych cieszy się coraz większym zainteresowaniem. W 2024 r. 30% Polaków deklaruje, że ma włączoną automatyczną synchronizację w chmurze na komputerze lub telefonie (w 2023r. było to 24%) – pytanie czy, aby na pewno odsetek ten w praktyce nie jest większy, a niektórzy użytkownicy po prostu nie są tego świadomi. Ponadto 17% deklaruje, że tworzy kopię zapasową co najmniej raz na trzy miesiące. Należy jednak zwrócić uwagę, że aż 15% nigdy nie robi żadnych kopii zapasowych, a 11% respondentów zabezpiecza tak swoje dane wyłącznie przy okazji wymiany komputera lub telefonu.

JAK CZĘSTO ROBISZ TZW. KOPIE ZAPASOWE SWOICH DANYCH ZGROMADZONYCH NA KOMPUTERZE LUB TELEFONIE?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

16/ W porównaniu do badania „Postawy Polaków wobec cyberbezpieczeństwa " z 2023r.

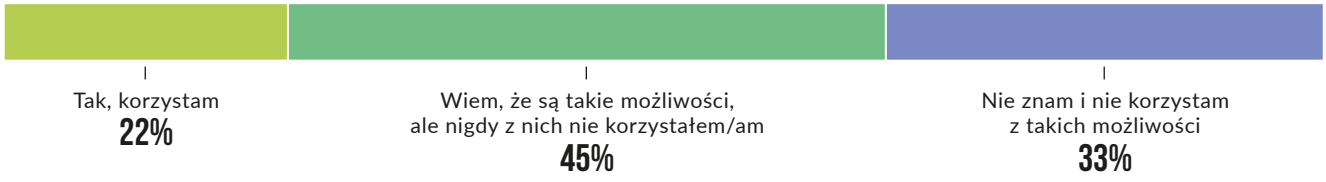
„Na podstawie przedstawionych wyników badania powstaje pytanie czy u podstaw pozytywnego wzrostu korzystania z chmury stoi rosnąca świadomość Polaków w zakresie zabezpieczenia danych, czy też domyślna konfiguracja wykorzystywanych urządzeń, która powoduje wykonywanie kopii bez lub z ograniczoną interakcją użytkownika. To drugie może oznaczać niedoszacowanie odsetka respondentów, bowiem dzięki rozwojowi technologii działania takie jak np. backup, stają się zautomatyzowane i wygodne, ale poza wiedzą użytkownika. To z kolei rodzi pewne ryzyko wykorzystania danych, czasem po nieświadomej akceptacji przetwarzającego. Dlatego kluczowe są nie tylko działania podnoszące poziom cyberbezpieczeństwa w społeczeństwie, ale także pobudzenie do myślenia nad celem, miejscem i aktualnością zabezpieczania danych. Chmura to w dużym uproszczeniu zasoby komputerowe kogoś innego, więc zanim przekażemy tam dane, należy zastanowić się nad ich poufnością i osiągalnością. Z drugiej strony, z badań wyłania się zatrważający brak lub nieregularność wykonywania kopii. Takie podejście do ochrony danych (także dostępowych) poszerza grono potencjalnych ofiar w kontekście możliwych cyberataków, awarii sprzętowych czy przypadkowej utraty danych. A zatem systemowa edukacja w zakresie cyberbezpieczeństwa powinna stać się priorytetem nowoczesnego państwa”

JAROSŁAW KOWALEWSKI,
DYREKTOR PIONU INFRASTRUKTUR
I TECHNOLOGII, ZAKŁAD USŁUG INFORMATYCZNYCH
NOVUM

AI – TECHNOLOGIA WSPARCIA CZY ZAGROŻENIE?

W ostatnim czasie nowe technologie utożsamiane są głównie z AI, czyli zastosowaniem sztucznej inteligencji w różnych branżach. Jej wykorzystanie w bankowości odbywa się nie tylko na poziomie zabezpieczeń, ale również w różnych aplikacjach i usługach bankowych usprawniających komunikację z klientem, jak np. chatboty czy wirtualni asystenci. Blisko połowa (45%) Polaków ma świadomość istnienia wirtualnego asystenta w swoim banku, ale jednak nie korzysta z tej usługi. Jedynie 22% respondentów wykorzystuje możliwość tego narzędzia do poszerzenia swojej wiedzy o bezpieczeństwie w bankowości elektronicznej.

CZY KORZYSTASZ Z WIRTUALNEGO ASYSTENTA LUB PRZESTRZENI TWOJEJ BANKOWOŚCI ELEKTRONICZNEJ/APLIKACJI BANKOWEJ, KTÓRE ZWIĄZANE SĄ Z PORADAMI I ZALECENIAMI CO DO BEZPIECZEŃSTWA?

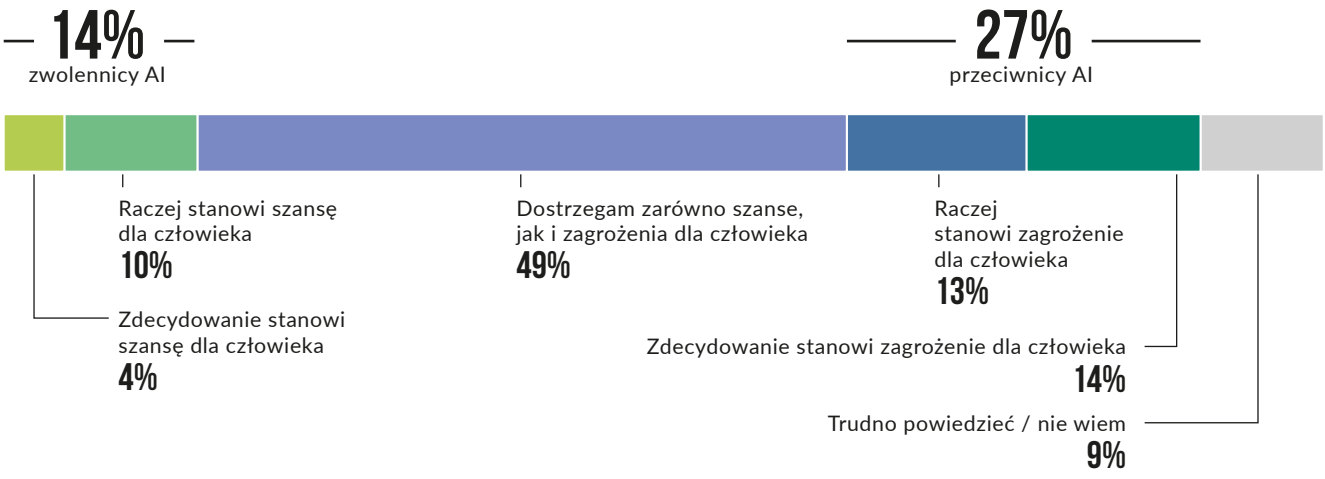


Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

Nieufność Polaków do sztucznej inteligencji jako wirtualnego asystenta nie oznacza całkowitego braku zaufania do tej technologii w szerszej ocenie – **blisko połowa badanych (49%) uważa, że sztuczna inteligencja jest zarówno szansą, jak i zagrożeniem dla człowieka**.

Niemniej jednak przeciwników AI jest prawie dwukrotnie więcej od zwolenników: 27% respondentów obawia się sztucznej inteligencji, a 14% uznaje ją za wsparcie dla człowieka.

JAKI JEST TWÓJ STOSUNEK DO AI (TJ. SZTUCZNEJ INTELIGENCJI)?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

Ponadto warto zauważyć, że nasze zaufanie do AI jest bezpośrednio powiązane z poziomem wykształcenia: osoby z wykształceniem wyższym są bardziej świadome zagrożeń, jakie może powodować sztuczna inteligencja – 27% respondentów po studiach ma ograniczone zaufanie do tej technologii, a wśród respondentów z wykształceniem podstawowym jest to 17%.

DEEPFAKE – JEDNO Z ZAGROŻEŃ W CYFROWYM ŚWIECIE WYGENEROWANYCH PRZEZ AI.

Wraz z intensywnym rozwojem narzędzi opartych na AI pojawiły się zupełnie nowe formy zagrożeń w przestrzeni cyfrowej. Jednym z nich jest tzw. deepfake, czyli metoda manipulacyjna, która polega na tworzeniu nieprawdziwych treści wizualnych i dźwiękowych poprzez wykorzystanie sztucznej inteligencji. Przykłady deepfake'ów wizualnych, czyli fałszywe zdjęcia wygenerowane przez AI:

FAŁSZYWE ZDJĘCIE KRĄŻĄCE W MEDIACH SPOŁECZNOŚCIOWYCH, PRZEDSTAWIAJĄCE PAPIEŻA FRANCISZKA W MARKOWEJ PUCHOWEJ KURTCE.

FAŁSZYWE ZDJĘCIA PRZEDSTAWIAJĄCE NIEPRAWDZIWĄ SCENĘ ARESZTOWANIA DONALDA TRUMPA

17/ Źródło: prezentacja NASK pt. „Bezpieczni w świecie dezinformacji" – materiał przygotowany w ramach projektu WIB pt. Bezpieczeństwo w Cyberprzestrzeni.
18/ Jw.

Część Polaków (29%) postrzega deepfake'i jako jedno z zagrożeń w cyfrowym świecie, ale jednocześnie mają problem z ochroną przed tą formą manipulacji. Bowiem według danych WIB tylko 12% badanych sprawdza pochodzenie zdjęć/obrazów ilustrujących informację w sieci. Tymczasem patrząc na sytuację globalną, jak wskazano w raporcie Google pt. „Cybersecurity Forecast 2024: Insights for future planning" przewiduje się nasilenie w najbliższym czasie dwóch rodzajów zagrożeń w sieci, tj. dezinformacji i właśnie deepfake'ów. Za pomocą AI można fabrykować treści, zdjęcia czy filmy i wykorzystywać tak stworzone materiały do kradzieży, oszustw i szantaży, ale też do wprowadzania w błąd i manipulowania wybranymi osobami, grupami, a nawet całą opinią publiczną.

Mimo, że według danych WIB, sceptyków wobec AI jest więcej niż zwolenników, to jej obecność w naszym codziennym życiu z pewnością będzie rosnąć. A to z kolei będzie wymagało od wszystkich użytkowników odpowiedniej świadomości, wiedzy i postaw.

ROZDZIAŁ V

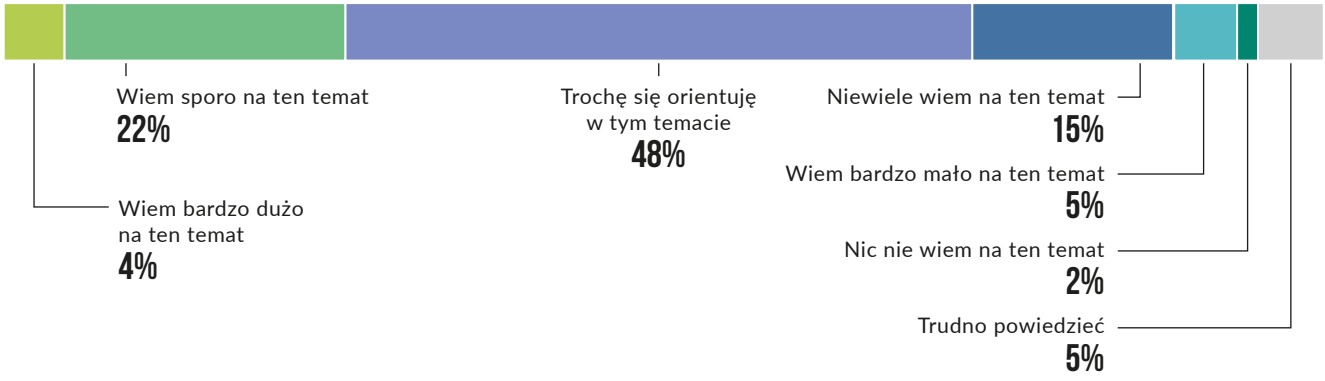
EDUKACJA, EDUKACJA i jeszcze raz EDUKACJA

POLACY ZBYT MAŁO WIEDZĄ O CYBERBEZPIECZEŃSTWIE I DEKLARUJĄ POTRZEBĘ WIĘKSZEJ EDUKACJI NA TEN TEMAT

We współczesnym świecie, w którym wiele spraw załatwiamy cyfrowo - począwszy od zakupów, bankowości, poprzez naukę, aż po spotkania towarzyskie i zawieranie znajomości - poziom wiedzy o cyberbezpieczeństwie powinien być wysoki. Niestety w Polsce wciąż pomimo pewnych pozytywnych zmian jest dużo do nadrobienia.

Blisko połowa Polaków (48%) deklaruje, że posiada pewną orientację w temacie cyberbezpieczeństwa, a 15% niewiele wie w tym zakresie. Natomiast tylko 22% badanych uważa, że wie sporo o bezpieczeństwie w przestrzeni cyfrowej, a 4% – bardzo dużo.

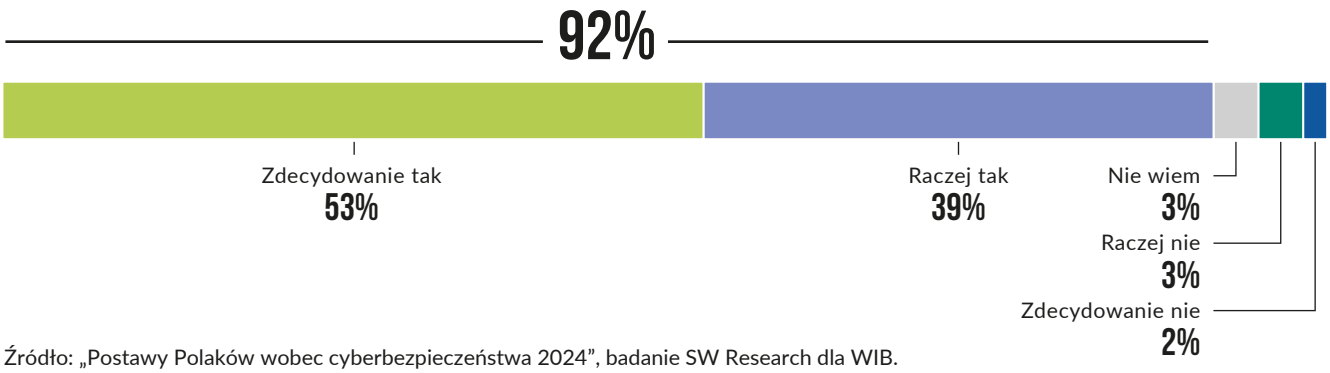
JAK OGÓLNIE OCENIASZ SWOJĄ WIEDZĘ W ZAKRESIE CYBERBEZPIECZEŃSTWA?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024”, badanie SW Research dla WIB.

Równocześnie badanie pokazuje, że Polacy mają świadomość swoich braków w wiedzy i deklarują chęć jej poszerzenia. Co istotne większość ankietowanych (92%) zauważa konieczność edukowania społeczeństwa na temat cyberbezpieczeństwa, w tym ponad połowa (53%) zdecydowanie widzi taką potrzebę.

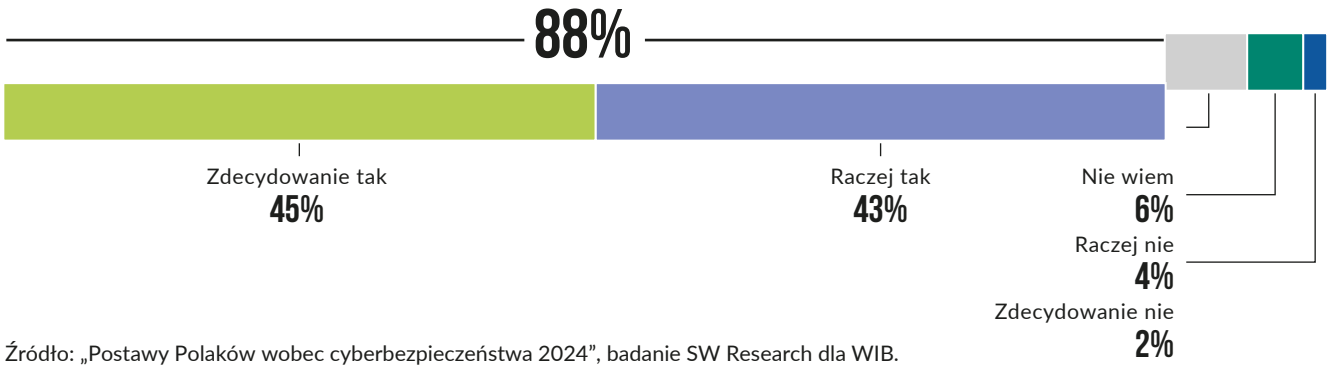
CZY UWAŻASZ, ŻE ISTNIEJE POTRZEBA WIĘKSZEJ EDUKACJI SPOŁECZNEJ NA TEMAT CYBERBEZPIECZEŃSTWA W POLSCE?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

Edukacja w zakresie bezpieczeństwa i higieny w przestrzeni cyfrowej powinna rozpoczynać się już od najmłodszych lat – 88% badanych uważa, że lekcje informatyki i innych przedmiotów w szkołach powinny w większym stopniu skupiać się na cyberbezpieczeństwie. Zdecydowane „tak" szkolnej edukacji wskazują osoby w wieku 35-45 lat (50%), co może oznaczać, że to głównie rodzice, którym zależy na bezpieczeństwie ich dzieci. Dorośli Polacy postrzegają szkołę jako instytucję, która w pierwszej kolejności powinna zadbać o edukację dzieci i młodzieży w zakresie cyberbezpieczeństwie.

CZY UWAŻASZ, ŻE LEKCJE INFORMATYKI I INNYCH PRZEDMIOTÓW W SZKOŁACH POWINNY W WIĘKSZYM STOPNIU SKUPIAĆ SIĘ NA CYBERBEZPIECZEŃSTWIE?



Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

ŻYCIE W CYFROWYM ŚWIECIE WYMAGA CIĄGŁEJ EDUKACJI W ZAKRESIE CYBERBEZPIECZEŃSTWA

Rozwój nowych technologii, w tym wspomnianej wcześniej sztucznej inteligencji, z jednej strony pomaga usprawniać pracę i życie współczesnego człowieka, ale z drugiej stwarza nowe możliwości cyberprzestępcom. Stąd tak istotne jest, aby wiedza o cyberbezpieczeństwie była stale przez nas aktualizowana. Zabezpieczenia, które dziś są uważane za skuteczne, wkrótce mogą okazać się niewystarczające. Prawie połowa Polaków (48%) ma świadomość tylko niektórych cyberzagrożeń, ale niestety nie ma wystarczającej wiedzy, w jaki sposób wykradzione przez przestępców dane mogą być wykorzystane przeciwko nim samym. Jedynie 36% ankietowanych deklaruje, że zna najczęściej kradzione typy danych oraz rozumie potencjalne skutki ich wykorzystania.

CZY JESTEŚ ŚWIADOMY/A, JAKIE TYPY DANYCH SĄ NAJCZĘŚCIEJ KRADZIONE PRZEZ CYBERPRZESTĘPCÓW I W JAKI SPOSÓB MOGĄ BYĆ WYKORZYSTANE?

Tak, znam najczęściej kradzione typy danych oraz znam i rozumiem potencjalne skutki ich wykorzystania
36%

Słyszałem/am o niektórych typach danych, które mogą być wykradzione, ale nie wiem, jak mogą być wykorzystane
48%

Nie mam pojęcia jakie typ danych są najczęściej kradzione przez cyberprzestępców ani jak mogą być wykorzystane
12%

Nie interesuje mnie to
4%

Źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2024", badanie SW Research dla WIB.

„Temat cyberbezpieczeństwa powinien pozostawać w zainteresowaniu wielu osób, a nie tylko tych, zajmujących się zawodowo zwalczaniem tych zjawisk. Problem cyberzagrożeń wzrasta i wzrastać będzie wraz z dalszym rozwojem nowych technologii. Warto jednak zauważyć, że problemem nie są nowe technologie same w sobie, a nieetyczne ich wykorzystanie. Żyjemy w cyfrowej globalnej wiosce, więc nieuniknione jest stałe śledzenie najnowszych metod cyberprzestępców i właściwe ich zrozumienie. Z jednej strony bycie bardziej świadomym pozwala lepiej zrozumieć potencjalne zagrożenia, z drugiej – buduje nasze zaufanie do nowych technologii, w tym np. do sztucznej inteligencji. Posiadane przez nas informacje, nasze dane, decyzje i interakcje w sieci są zagrożone tym bardziej, im częściej pozostajemy online. Edukacja w zakresie świadomości zagrożeń, regularne ostrzeganie i docieranie do jak największych grup odbiorców, pozwoli skuteczniej chronić Internautów. Celem ekspertów od cyberbezpieczeństwa powinna być również praca dydaktyczna, również w zakresie bezpieczeństwa naszego portfela. Mówi się, że najsłabszym ogniwem jest człowiek. Warto wierzyć, że może być odwrotnie – świadomy, odpowiedzialny człowiek może być najmocniejszym ogniwem w walce z cyberprzestępczością"

PRZEMYSŁAW PORĘBA, EKSPERT DS. CYBERBEZPIECZEŃSTWA,
POLSKI STANDARD PŁATNOŚCI - BLIK.

ROZDZIAŁ **VI**

ABC Cyberbezpieczeństwa

Dane WIB pokazują, że rozpoznawanie cyberzagrożeń i zapobieganie im nie jest obecnie łatwym zadaniem. Podnoszenie świadomości w tym zakresie jest konieczne, mając na uwadze postępującą cyfryzację kraju, a co za tym idzie również gwałtowny wzrost liczby cyberincydentów i nowego rodzaju zagrożeń, z którymi coraz częściej mamy do czynienia. Stąd poniżej przedstawiliśmy 10 podstawowych zasad bezpiecznego funkcjonowania w przestrzeni cyfrowej i korzystania z bankowości elektronicznej. **Przeczytaj ABC Cyberbezpieczeństwa, zapamiętaj i wdrażaj w życie!**

1. CHROŃ SWOJE DANE OSOBOWE I WIZERUNEK!

Uważaj na to, jakie treści i zdjęcia publikujesz w Internecie! Nie udostępniaj w przestrzeni cyfrowej, w tym w mediach społecznościowych swoich danych: kontaktowych (adresu zamieszkania, nr telefonu – z wyjątkiem przypadku dwuskładnikowego uwierzytelniania) i tych poufnych typu PESEL czy numer dokumentu z twoim wizerunkiem.

Pochwalenie się zdjęciem w sieci „świeżo" otrzymanym dowodem osobistym czy prawem jazdy albo biletem lotniczym z danymi osobowymi, to tylko podstawowe przykłady niebezpiecznych zachowań – **takie postępowanie może skutkować kradzieżą twoich danych przez cyberprzestępców w celu wyłudzania pieniędzy.**

Udostępnione twoje zdjęcie lub kogoś bliskiego/znajomego w mediach społecznościowych **może zostać użyte np. do oszustw z wykorzystaniem deepfake** – przykładowo sztuczna inteligencja potrafi „wykraść" fotografię z twojego profilu, przywłaszczyć wizerunek osoby i wykorzystać zdjęcie do fałszywej zbiórki pieniędzy.

Bądź ostrożny na połączenia telefoniczne z nieznanych numerów – przestępcy mogą dzwonić i podszywać się pod osobę zaufania publicznego (np. policjanta, lekarza, pracownika ZUS) i/lub rzekomych przedstawicieli banków w celu wyłudzenia danych osobowych albo danych do twojego konta bankowego.

Warto wiedzieć, że istnieje tzw. spoofing (tj. fałszowanie numeru telefonu wybranej osoby czy instytucji) – przestępcy wykorzystując technologię i różne narzędzia internetowe są w stanie podszyć się pod każdy numer – stąd pamiętaj, że osoba, która do Ciebie dzwoni nie musi być tym, za kogo się podaje!

Zawsze zatem weryfikuj osobę, która do Ciebie dzwoni: rozłącz się, samodzielnie wybierz numer na klawiaturze telefonu i zadzwoń do placówki banku/miejsca zatrudnienia osoby dzwoniącej w celu potwierdzenia czy taka osoba rzeczywiście jest pracownikiem danego miejsca.

Nigdy nie podawaj przez telefon numerów kart płatniczych czy danych do logowania do swojej bankowości elektronicznej, a bez weryfikacji osoby dzwoniącej – nr PESEL.

Nie działaj pod presją czasu: uważaj na emaile, SMS-y, strony internetowe, aplikacje i telefony, które skłaniają do natychmiastowego działania i podawania danych.

2. AKTUALNY PROGRAM ANTYWIRUSOWY JEST OBOWIĄZKIEM DLA KAŻDEGO!

Używaj antywirusa nie tylko na komputerze/laptopie, ale **zabezpieczaj również inne urządzenia, takie jak: telefon komórkowy, tablet, smartwatch**.

Aby ochrona była skuteczna, regularnie aktualizuj swój sprzęt i pobieraj bieżące aktualizacje programów.

3. ZAWSZE USTAWIAJ SILNE HASŁA ZŁOŻONE Z CIĄGU ZNAKÓW!

Tworząc hasło pamiętaj, że obecnie bezpieczne hasło składa się już **nawet z 15 znaków** (a nawet więcej), **w których są małe i wielkie litery, liczby i znaki specjalne.**

Unikaj haseł zawierających dane osobowe (typu imię i nazwisko, data i miejsce urodzenia). **Lepiej tworzyć długie hasła oparte o ciąg skojarzeń, pełne zdanie lub wyobrażonych scenach**, aby zwiększyć ich siłę przy jednoczesnym zachowaniu łatwości zapamiętania.

Jeśli nie jesteś w stanie wymyślić skomplikowanego hasła – stosuj generatory haseł, które wygenerują je za Ciebie w formie odpowiednio bezpiecznej.

Używaj różnych haseł do każdej usługi czy serwisu!

Stosuj uwierzytelnianie dwuskładnikowe / dwuetapowe, tj. oprócz stworzenia silnego hasła, ustaw drugi etap zabezpieczający logowanie, np. dodatkowe hasło uwierzytelniające w SMS.

4. NIE ZAPOMINAJ O WYLOGOWANIU SIĘ!

Zawsze po zakończonej transakcji, przeczytaniu emaili lub innej czynności na jakimkolwiek internetowym koncie - wyloguj się! Ta czynność po zakończeniu pracy z danym systemem, aplikacją lub usługą powinna być naturalnym odruchem dla każdego. Jeśli pozostajesz zalogowany dłużej niż potrzebujesz, stwarzasz możliwość nadużycia, włamania czy przejęcia konta.

5. BĄDŹ OSTROŻNY W KWESTII BANKOWOŚCI ELEKTRONICZNEJ!

Stosuj się do ustalonych zasad bezpieczeństwa zamieszczonych na stronie twojego banku. Jeśli coś wzbudzi twój niepokój (np. niespodziewany telefon z banku, nieautoryzowane przez ciebie wydatki na koncie), natychmiast skontaktuj się z obsługą klienta.

Dokonuj płatności tylko z własnego komputera lub telefonu zabezpieczonego programem antywirusowym.

Używaj dwuskładnikowego uwierzytelniania transakcji, np. poprzez autoryzację mobilną, hasło wysłane w SMS-ie – wówczas zawsze dokładnie czytaj informację zawartą w aplikacji mobilnej lub SMS-ie, tj. nr konta odbiorcy i kwotę transakcji.

Najlepiej nie wchodź na stronę banku z linku w wyszukiwarce, lecz wpisuj adres ręcznie.

Zwracaj uwagę na prawidłowość adresu strony www twojego banku (tj. czy nie ma literówki lub czy nie zostały dodane do adresu www dodatkowe literki/cyfry/znaki specjalne) – pamiętaj, że kłódka przy adresie www nie oznacza, że strona jest całkowicie bezpieczna (kłódka oznacza tylko, że dane połączenie internetowe jest szyfrowane).

Pamiętaj, że przedstawiciel banku (lub innej instytucji finansowej) nigdy nie poprosi cię o login i hasło do konta bankowego, czy też inne poufne dane, np. kod PIN do karty płatniczej.

6. ZWRACAJ UWAGĘ NA JAKIE STRONY INTERNETOWE WCHODZISZ I ICH ADRESY!

Zważaj czy wchodzisz na szyfrowaną stronę internetową, tj. czy adres strony posiada na początku https// – oznacza to, że dane i operacje wykonywane na takiej stronie są zabezpieczone dzięki szyfrowaniu.

Pamiętaj jednak, że samo https i kłódka na początku adresu strony www, nie oznacza, że witryna jest całkowicie bezpieczna – trzeba zwracać uwagę na poprawność całego adresu www, szczególnie na jego zakończenie, tj. czy ma końcówkę pl/com!

Warto również korzystać z narzędzi do sprawdzania witryn internetowych pod kątem wirusów, np. z serwisu VirusTotal, który umożliwia wykrycie „zaszytego" wirusa na danej stronie.

7. UWAŻAJ NA PRZESYŁANE WIADOMOŚCI I ZAŁĄCZNIKI ZAWARTE W EMAILACH, SMS-ACH LUB KOMUNIKATORACH

Nigdy nie otwieraj wiadomości i dołączonych do nich załączników od nieznanych nadawców.

Bądź uważny na linki i załączniki w otrzymywanych wiadomościach nawet od osób zaufania publicznego czy instytucji publicznych – cyberprzestępcy mogą tworzyć fałszywe (ale wyglądające na prawdziwe i wiarygodne) emaile, SMS-y, komunikaty, w których przy pomocy wzbudzenia niepokoju, będziesz namawiany do kliknięcia w link czy załącznik.

(MESSENGER, WHATSAPP) **OD NIEZNANYCH, ALE TEŻ ZNANYCH NADAWCÓW – TO MOŻE BYĆ PHISHING!**

Najpopularniejsze tematy fałszywych wiadomości to:
- niezapłacona faktura,
- informacje o brakującej dopłacie, np. do wysyłanej paczki, za prąd/gaz itp.
- problemy z kontem bankowym (np. informacje o zablokowanym koncie lub podejrzanych aktywnościach na koncie),
- wygrane w loterii, zniżki i kupony do popularnych sklepów,
- problemy z wypłaceniem dodatkowych świadczeń.

Pamiętaj również, że w załącznikach (najczęściej o rozszerzeniu .exe lub w formie spakowanych plików rar/zip) **mogą być ukryte złośliwe oprogramowania i wirusy**.

8. ZAWSZE TWÓRZ KOPIE ZAPASOWE!

Nie zapominaj o tworzeniu kopii zapasowych danych, in. stosuj tzw. backup – zabezpieczasz w ten sposób swoje pliki na wypadek ich utraty bądź uszkodzenia.

9. UWAŻAJ NA FAKE NEWSY I DEZINFORMACJĘ!

Nie wierz we wszystko, co czytasz w Internecie – miej świadomość, że w sieci i w mediach społecznościowych umieszcza się również nieprawdziwe informacje i sfabrykowane opinie.

Nie ograniczaj się do czytania tytułów/nagłówków wiadomości, tylko zapoznaj się z całym tekstem. Unikaj klikalnych nagłówków (tzw. clickbaitów).

Potwierdzaj przeczytaną informację w Internecie w kilku źródłach oraz korzystając z wiarygodnych i rzetelnych źródeł informacji, tj. np. portale internetowe mediów tradycyjnych (gazet, agencji prasowych).

Rozważnie komentuj i reaguj na treści pojawiające się w Internecie, zwłaszcza w mediach społecznościowych. Miej świadomość, że w dyskusjach internetowych mogą uczestniczyć tzw. „trolle" (tj. osoby hejtujące, działające na zlecenie dezinformatora), a także zautomatyzowane narzędzia tzw. „boty".

10. ZDOBYWAJ I POSZERZAJ SWOJĄ WIEDZĘ NA TEMA CYBER-BEZPIECZEŃSTWA!

Pamiętaj, że cyberprzestępcy nie stoją w miejscu, asymilują się ze światem współczesnego cyfrowego świata, tworząc nowe sposoby i formy oszustw – dlatego warto na bieżąco interesować się zagadnieniami cyberbezpieczeństwa oraz zdobywać wiedzę w tym zakresie. **Naprzeciw potrzebie edukacji w zakresie bezpieczeństwa w przestrzeni cyfrowej wychodzi projekt Fundacji Warszawski Instytut Bankowości „Bezpieczeństwo w Cyberprzestrzeni" www.cyber.wib.edu.pl**

ŹRÓDŁA I AUTORZY RAPORTU

ŹRÓDŁA RAPORTU:

1. **www.cashless.pl**:
   https://www.cashless.pl/15476-apple-pay-google-pay-liczba-platnosci-1-kw-2024

2. **CERT Polska**
   www.cert.pl: https://cert.pl/hasla/

3. **CERT Orange** www.cert.orange.pl:
   https://cert.orange.pl/warto-wiedziec/bezpieczne-hasla/

4. **NASK-PIB „Raport roczny z działalności CERT Polska 2023", publikacja z dn. 17.04.2024r.**:
   https://www.nask.pl/pl/raporty/raporty/5381,RAPORT-CERT-2023.html

5. **Raport Fundacji Polska Bezgotówkowa i Spotdata „Przyszłość płatności. W stronę bezpiecznego cyfrowego świata", listopad 2023r.**:
   https://polskabezgotowkowa.pl/badania-i-analizy/przyszlosc-platnosci-w-strone-bezpiecznego-cyfrowego-swiata/

6. **Raport ZBP „Netbank. Bankowość internetowa i mobilna, płatności bezgotówkowe", dane za I kwartał 2024r.:**
   https://www.zbp.pl/getmedia/af62d399-e9ff-42ff-9f52-d3adbef3e312/czerwiec_Netbank_2024

7. **Raport z badania WIB i ZBP „Postawy Polaków wobec cyberbezpieczeństwa 2023"**:
   https://cyber.wib.edu.pl/wp-content/uploads/2024/02/RAPORT_Postawy-wobec-cyber_2023.pdf

ZESPÓŁ REDAKCYJNY RAPORTU:

Aleksandra Czyrkowska,
Marta Jaros

O PROJEKCIE EDUKACYJNYM BEZPIECZEŃSTWO W CYBERPRZESTRZENI

Ogólnopolski projekt „Bezpieczeństwo w Cyberprzestrzeni" Fundacji Warszawskiego Instytutu Bankowości został zainicjowany w ramach porozumienia z 2017 r. i jest z sukcesami realizowany w ramach sektorowego Programu „Bankowcy dla Edukacji" – jednego z największych programów edukacji finansowej w Europie.

Projekt realizowany jest wspólnie z Partnerami: merytorycznym – NASK oraz wspierającymi: Allegro, BLIK, ING Bank Śląski, Santander Bank Polska, VISA, DAGMA Bezpieczeństwo IT, ESET, Zakład Usług Informatycznych NOVUM.

CELE PROJEKTU:

- edukowanie Polaków w zakresie umiejętnego i bezpiecznego korzystania z nowoczesnych narzędzi cyfrowych, w tym bankowości elektronicznej

- podnoszenie poziomu wiedzy na temat cyberzagrożeń, a także w zakresie dezinformacji

- kształtowanie właściwych postaw w dziedzinie cyberbezpieczeństwa oraz popularyzację gospodarki elektronicznej.

GRUPY DOCELOWE:

W RAMACH PROJEKTU „BEZPIECZEŃSTWO W CYBERPRZESTRZENI" REALIZOWANYCH JEST WIELE AKTYWNOŚCI, W TYM KLUCZOWE DZIAŁANIA STANOWIĄ:

- lekcje, wykłady, webinary i szkolenia o cyberbezpieczeństwie,
- testy wiedzy pt. Cyber Geniusz (edycja dla uczniów i studentów)
- sesje tematyczne o cyberbezpieczeństwie podczas różnych wydarzeń, w tym Kongresu Edukacji Finansowej i Przedsiębiorczości
- audycje radiowe/podcasty,
- raporty i badania,
- publikacje i materiały edukacyjne o cyberbezpieczeństwie,
- filmy i kampanie edukacyjne

PROJEKT DOTARŁ DO 1,5 MILIONA ODBIORCÓW, W TYM BEZPOŚREDNIO DO:

ponad **260 tys.** uczniów

ponad **120 tys.** studentów

pośrednio/bezpośrednio do **219 tys.** seniorów

CHCESZ WIEDZIEĆ WIĘCEJ O BEZPIECZEŃSTWIE W INTERNECIE, MEDIACH SPOŁECZNOŚCIOWYCH I BANKOWOŚCI ELEKTRONICZNEJ?

Zostań aktywnym uczestnikiem projektu
Bezpieczeństwo w Cyberprzestrzeni!
Wejdź na stronę **www.cyber.wib.edu.pl**,
zdobądź wiedzę i bądź bezpieczny!

MASZ PYTANIA WS. RAPORTU „CYBERBEZPIECZNY PORTFEL" LUB O PROJEKCIE BEZPIECZEŃSTWO W CYBERPRZESTRZENI?

SKONTAKTUJ SIĘ Z KOORDYNATORKĄ PROJEKTU:

Aleksandra Czyrkowska
Fundacja Warszawski Instytut Bankowości
email: aczyrkowska@wib.org.pl
tel. (+48) 791 502 298

WIĘCEJ INFORMACJI I MATERIAŁÓW EDUKACYJNYCH ZNAJDZIESZ RÓWNIEŻ NA STRONACH:

Warszawskiego Instytutu Bankowości: **www.wib.org.pl**
Programu „Bankowcy dla Edukacji": **www.bde.wib.org.pl**