RAPORT

Cyberbezpieczny portfel

publikacja Warszawskiego Instytutu Bankowości
we współpracy ze Związkiem Banków Polskich

Edycja IV
lipiec **2022 r.**

WARSZAWSKI INSTYTUT BANKOWOŚCI 30 LAT
BEZPIECZEŃSTWO W CYBERPRZESTRZENI
BANKOWCY DLA EDUKACJI program sektorowy
ZWIĄZEK BANKÓW POLSKICH

SPIS TREŚCI

WPROWADZENIE

Szanowni Państwo,

raport „Cyberbezpieczny portfel" to ciekawa publikacja skłaniająca do pogłębienia swojej wiedzy w zakresie właściwych postaw w obszarze cyberbezpieczeństwa oraz funkcjonowania najnowszych trendów w branży finansowej ze szczególnym uwzględnieniem sektora bankowego. Rozwój nowoczesnych technologii jest obecnie globalny i niezwykle szybki i wywiera duży wpływ na bezpieczeństwo banków. Celem utrzymania odpowiedniego poziomu bezpieczeństwa, banki muszą chronić swoje zasoby przed cyber atakami, kradzieżą danych, awariami, a jednocześnie zwiększać dostępność danych i aplikacji dla klientów. To trudne zadanie i wymaga odpowiednich narzędzi, wiedzy i kwalifikacji.

Raport „Cyberbezpieczny portfel" to cykliczna publikacja Warszawskiego Instytutu Bankowości i Związku Banków Polskich, która zawiera nie tylko analizę sytuacji, ale również zbiór prostych, podstawowych porad, które zwiększą bezpieczeństwo naszego portfela, a także pozwolą ochronić nasze dane osobowe przed ich wyłudzeniem i bezprawnym wykorzystaniem. Raport oparty jest o wyniki corocznego badania „Postawy Polaków wobec cyberbezpieczeństwa", przeprowadzonego w czerwcu br. na zlecenie WIB przez Instytut Badań Pollster.

Analizując wszystkie dane zawarte w niniejszej, czwartej edycji raportu „Cyberbezpieczny portfel" należy pamiętać, że cyberprzestrzeń jest obszarem ulegającym niezwykle dynamicznym przemianom. Zarówno w sferze rozwiązań i możliwości technologicznych, jak i technik stosowanych przez przestępców. Dlatego też, wnioski z badań uzupełniamy o części poradnikową i edukacyjną, które zawierają zbiór zasad podnoszących poziom naszego bezpieczeństwa przy poruszaniu się w cyberprzestrzeni, w tym bankowości elektronicznej.

Zachęcamy do zapoznania się z raportem i życzymy miłej i ciekawej lektury!

Fundacja Warszawski Instytut Bankowości

Publikacja oparta jest o dane własne Warszawskiego Instytutu Bankowości, zebrane na podstawie badań opinii społecznej, w tym badania „Postawy Polaków wobec cyberbezpieczeństwa", przeprowadzonego w czerwcu br. przez pracownię Pollster metodą CAWI w reprezentatywnej grupie dorosłych Polaków na próbie badawczej 1000 osób.

1 NA POCZĄTEK KILKA LICZB

NA POCZĄTEK KILKA LICZB

73% Polaków uważa, że odpowiedzialność za bezpieczeństwo finansowych usług elektronicznych ponosi bank

71% Polaków czuje się bezpiecznie korzystając z bankowości elektronicznej (konto internetowe/aplikacja/karta płatnicza)

57% Polaków uznaje banki jako liderów w zakresie cyberbezpieczeństwa

55% Polaków uważa, że banki w obszarze cyberbezpieczeństwa stosują wysokie standardy i raczej czują się spokojni o bezpieczeństwo zgromadzonych oszczędności

51% Polaków deklaruje, że posiada zainstalowane i aktualne oprogramowanie antywirusowe na telefonie komórkowym

44% Polaków stosuje kod PIN jako rodzaj zabezpieczenia/ blokady ekranu w swoim telefonie

źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

2 CYBERBEZPIECZEŃSTWO W BANKOWOŚCI

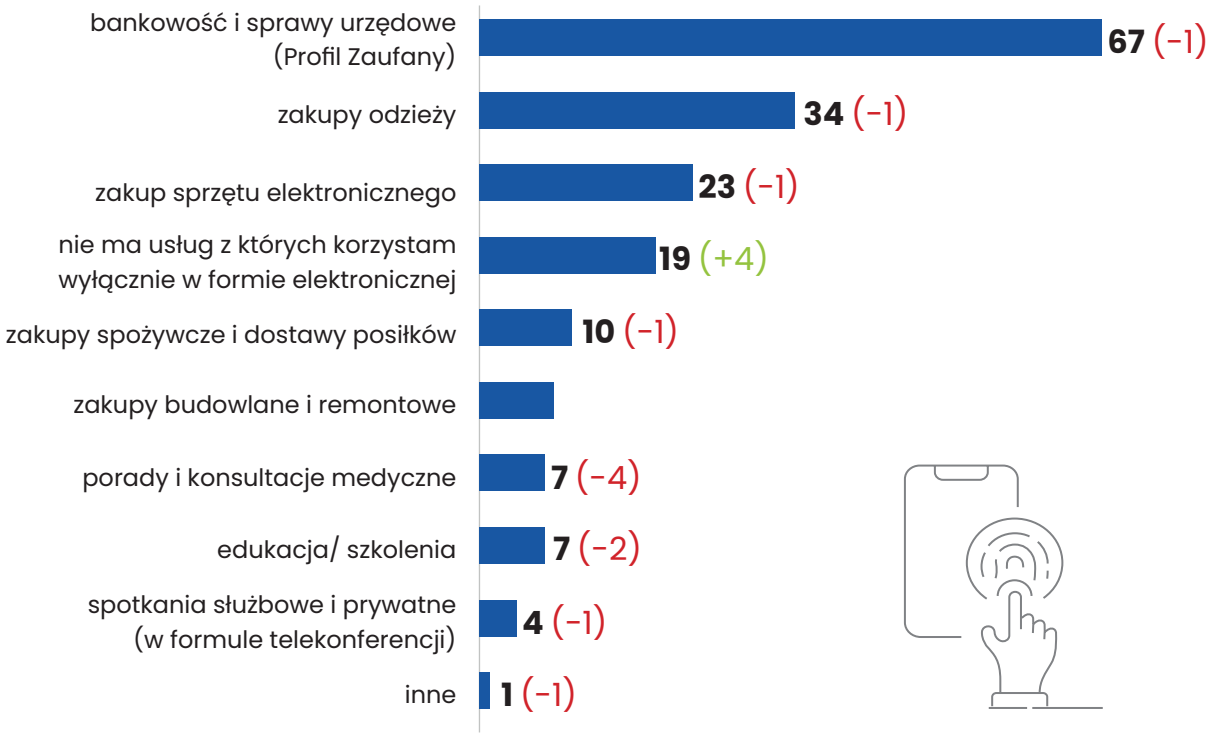
CYBERBEZPIECZEŃSTWO W BANKOWOŚCI

Transakcje bankowe przez internet lub płatności bezgotówkowe przy użyciu telefonu czy smartwatcha to już codzienność, która sprawia, że mnożą się wyzwania związane z ochroną danych i bezpieczeństwem w sieci. Bankowość detaliczna i korporacyjna wciąż rozwija swoje cyfrowe oblicze i wydaje się, że czasy miłośników pieczątki z oddziału przeminęły bezpowrotnie.

Coraz chętniej do sieci przenosimy także zakupy, a zwrot ku e-commerce widać jak na dłoni. Najczęściej tylko w internecie kupujemy: odzież (34 proc.), sprzęt elektroniczny (23 proc.), a także produkty spożywcze i posiłki na zamówienie (10 proc.). Niedziwne więc, że zarówno duże firmy, jak i małe biznesy stawiają na cyfrowe kanały sprzedaży. Wśród nich są także banki, które z powodzeniem rozszerzają dostępność swoich usług w internecie. Nieco ponad 2/3 Polaków (67 proc.), mając styczność z urzędami i swoim bankiem, najczęściej korzysta z ich usług wyłącznie online. Co ciekawe, wskaźnik osób korzystających z usług bankowych przez internet jest najniższy w grupie wiekowej 18-24 (60 proc.), a najwyższy (75 proc.) w grupie respondentów po 65. roku życia.

Z których usług najczęściej korzystasz w formie wyłącznie elektronicznej?

dane w % (porównanie rok do roku)



źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

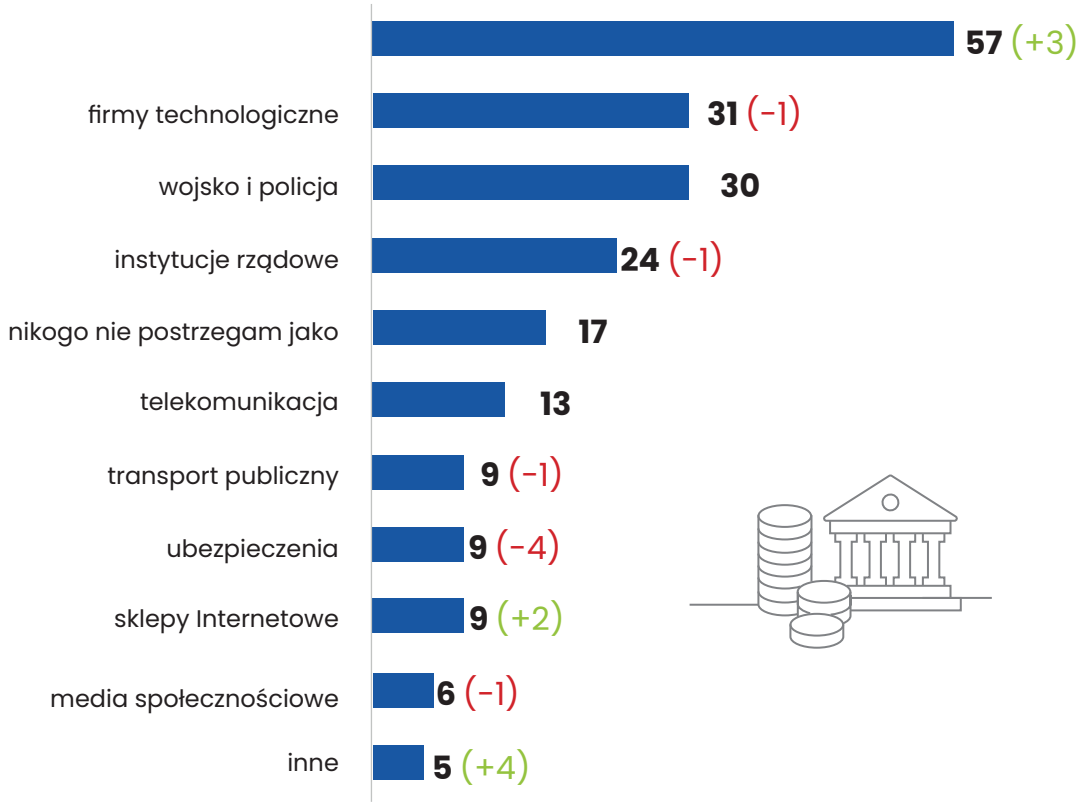
Wysoki wskaźnik korzystających z bankowości elektronicznej odzwierciedlają badania poziomu zaufania do instytucji finansowych. W zakresie cyberbezpieczeństwa jako liderów Polacy niezmiennie postrzegają sektor bankowy – uważa tak prawie 57 proc. respondentów. Wraz z postępem digitalizacji, wysokie jest również zaufanie do firm technologicznych – 31 proc. (od 2020 r. wzrost o 9 p. p.), a także do służb mundurowych – 30 proc. i instytucji rządowych – 24 proc. W przypadku dwóch ostatnich, w ciągu dwóch lat, zanotowano jednak nieznaczne spadki zaufania: wojsko i policja – 9 p. p., instytucje rządowe – 7 p. p. Spadek zaufania zanotował także transport lotniczy – 9 proc. (spadek o 7 p. p.).

Z kolei w gronie obszarów, których Polacy nie darzą szczególnym zaufaniem znalazły się media społecznościowe – tylko 5 proc. ankietowanych uznało je za liderów zaufania w zakresie cyberbezpieczeństwa – oraz sklepy internetowe – 6 proc.

Znaczna część Polaków ocenia, że banki jako liderzy zaufania stosują wysokie (55 proc.) lub najwyższe standardy (15 proc.). Respondenci czują się zatem względnie spokojni o bezpieczeństwo powierzonych pieniędzy. Tylko 2 proc. z nich poddaje pod wątpliwość bezpieczeństwo swoich danych i wskazuje, że instytucje finansowe mają słabe zabezpieczenia. Zaufanie do banków widać także w badaniach o aplikację bankową i konto internetowe. Prawie ¾ ankietowanych raczej czuje się bezpiecznie korzystając z cyfrowych usług oferowanych przez swój bank. Dodatkowo, aż 17 proc. jest przekonana o swoim poczuciu bezpieczeństwa.

Którą z poniższych branż i instytucji postrzegasz jako liderów w zakresie cyberbezpieczeństwa?

dane w % (porównanie rok do roku)

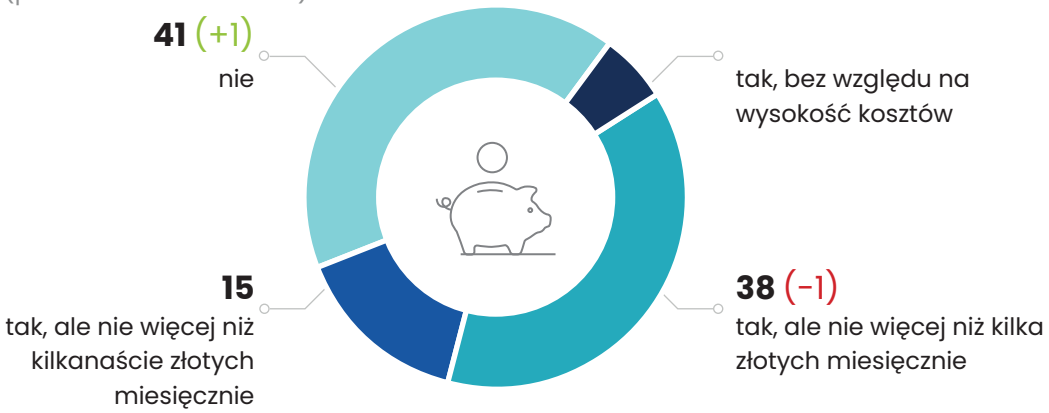


źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Wygląda na to, że banki – w oczach swoich klientów – nie odstępują na krok szybkiego tempa digitalizacji i skutecznie odpowiadają na „cyberwyzwania" współczesności. Postrzegając jako dobry swój poziom cyberbezpieczeństwa w bankowości, konsumenci w znacznej części nie są skłonni dodatkowo płacić za wzrost poziomu zabezpieczeń – tak zadeklarowało 41 proc. respondentów. Pozostała część mogłaby zapłacić nie więcej niż kilka (38 proc.) lub kilkanaście złotych miesięcznie (15 proc.).

Czy jesteś skłonny/a do ponoszenia dodatkowych, stałych miesięcznych kosztów podnoszących poziom zabezpieczeń Twojego cyberbezpieczeństwa w tym np. internetowego konta bankowego lub bankowej aplikacji mobilnej?

dane w % (porównanie rok do roku)



źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Takie odpowiedzi w dużej mierze to naturalna konsekwencja opinii, według której Polacy w większości uważają, że odpowiedzialność za bezpieczeństwo finansowych usług elektronicznych spoczywa na barkach usługodawców, a nie ich samych. Respondenci wskazują, że odpowiedzialność za bezpieczeństwo to zadanie banku (73 proc.), instytucji płatniczych (25 proc.), operatorów komórkowych lub internetowych (17 proc.) oraz firm rozliczających transakcję (11 proc.). Tylko 3 na 10 respondentów deklaruje, że to klient powinien wziąć na siebie odpowiedzialność za bezpieczeństwo usług finansowych w sieci, co z punktu widzenia tego, że to użytkownik jest najważniejszym bo ostatnim ogniwem bezpieczeństwa, wzbudza i będzie wzbudzać niepokój wśród ekspertów.

Odpowiedzialność za bezpieczeństwo finansowych usług elektronicznych ponosi Twoim zdaniem przede wszystkim

dane w % (porównanie rok do roku)

źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Powyższe wskazania wypadają spójnie na tle opinii o opłatach za podwyższone cyberbezpieczeństwo. Konsumenci deklarują w badaniach, że wypełniają zalecenia bankowe dotyczące bezpieczeństwa i widocznie nie widzą sensu ponoszenia dodatkowych opłat z tego tytułu.

Ponad 70 proc. Polaków twierdzi bowiem, że nie otwiera załączników lub nie klika w linki od nieznanych nadawców. Ponadto, przeszło połowa z nas deklaruje, że nie podaje swoich danych takich jak numeru telefonu lub adresu w mediach społecznościowych i na różnego rodzaju forach.

Co drugi z ankietowanych twierdzi również, że zwraca należytą uwagę na symbol kłódki i https:// przed adresem strony internetowej banku. Aż 70 proc. nie klika w podejrzane linki i załączniki, a 62 proc. wskazało, że nie przechowuje danych do logowania do bankowości w portfelu lub smartfonie. Wzmożona ostrożność przed wpisaniem haseł, pozwala na uniknięcie przekazania danych bankowych oszustom podszywającym się pod bank. Polacy są więc świadomi zagrożeń czyhających w cyberprzestrzeni i – jak w większości deklarują – podejmują odpowiednie kroki w celu ich zniwelowania. Zaledwie 5 proc. ankietowanych twierdzi, że nie stosuje się do żadnych wytycznych poprawiających bezpieczeństwo, przekazywanych przez banki w swoich strategiach komunikacji. W tym miejscu jednak należy wskazać, ze jednak wciąż istotna część klientów, nie jest świadoma lub zapomina o tych kilku podstawowych zasadach bezpieczeństwa. Ponadto, wraz z rozwojem usług cyfrowych, niestety rozwijają się również metody przestępcze i nawet jeśli dziś czujemy się odpowiednio wyedukowani, to już w niedalekiej przyszłości, nie rozwijając tej wiedzy, możemy stać się łatwym celem ataków cyberprzestępców.

Zaznacz do których zaleceń bankowych się stosujesz

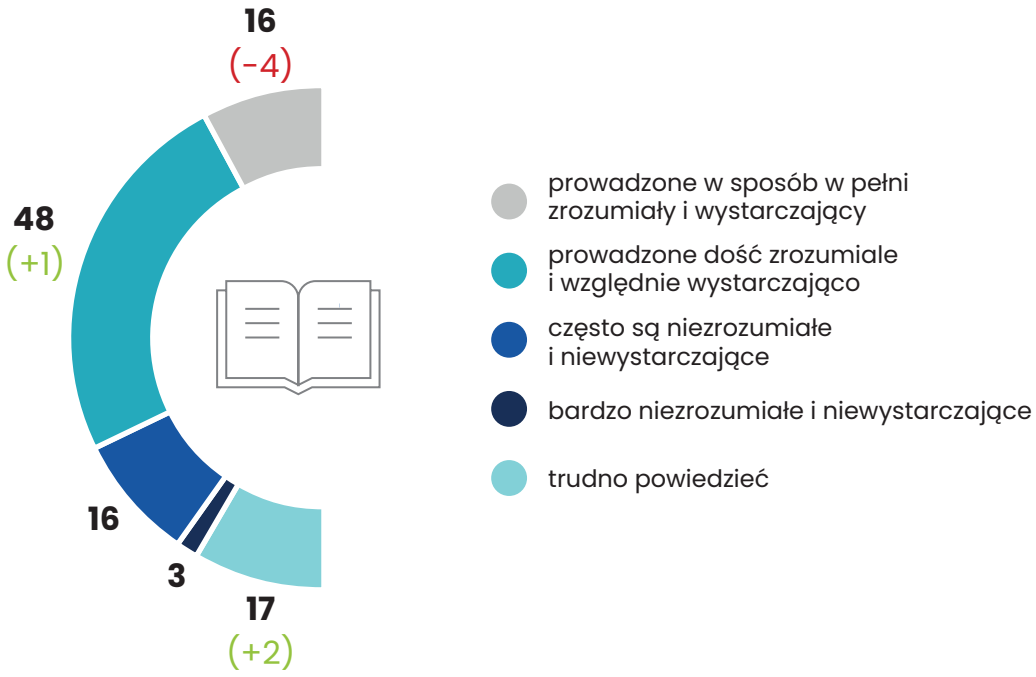
dane w % (porównanie rok do roku)

źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Niski odsetek tych, którzy nie uważają w sieci to dowód na to, że działania informacyjne i edukacyjne banków w zakresie cyberbezpieczeństwa działają. Prawie połowa respondentów (49 proc.) stwierdziła, że aktywności podejmowane przez banki w celu upowszechnienia podstawowej wiedzy o przeciwdziałaniu zagrożeniom w sieci są prowadzone w sposób dość zrozumiały i względnie wystarczający. Niepokoi jednak fakt, że odnotowano relatywnie wysoki odsetek osób, które uważają odwrotnie (16 proc.) oraz tych, które nie były w stanie jednoznacznie wypowiedzieć się w tej kwestii (17 proc.).

Czy działania informacyjne i edukacyjne banków w obszarze cyberbezpieczeństwa są...

dane w % (porównanie rok do roku)



źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

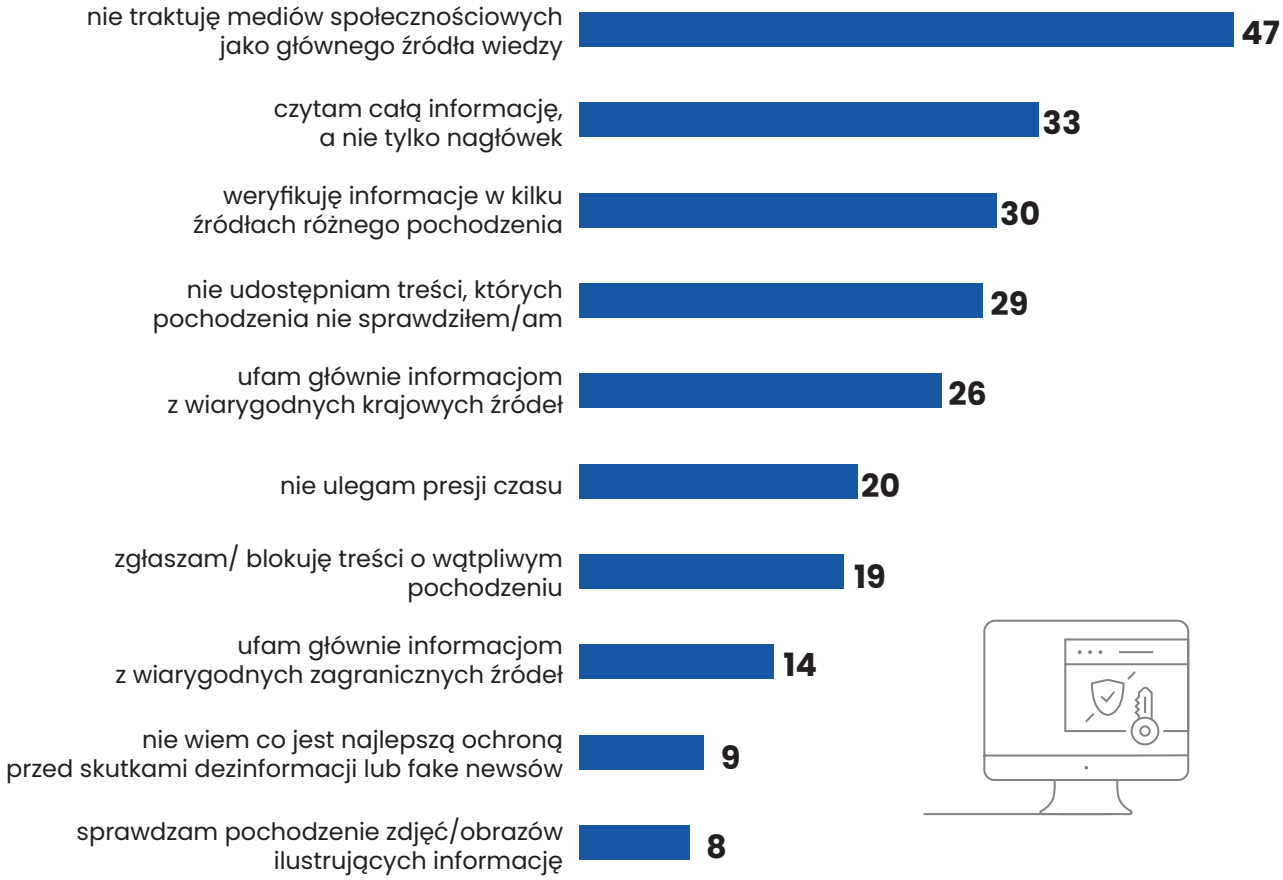
Wiele jest zatem do udoskonalenia, a edukację ekonomiczną w zakresie cyberbezpieczeństwa powinny prowadzić wszystkie instytucje finansowe, które mają na względzie bezpieczeństwo danych swoich klientów.

Nie jest tak źle w kontekście unikania szerzenia dezinformacji i przeciwdziałaniu rozprzestrzeniania się fakenewsów. Co czwarty respondent ufa informacjom z wiarygodnych krajowych źródeł, a tylko 14 proc. z zagranicznych źródeł tego typu. Z kolei 33 proc. ankietowanych stwierdziło, że czytanie informacji nie ogranicza tylko do nagłówka, a niewiele mniej, bo 30 proc. weryfikuje przeczytane informacje w kilku źródłach i nie ulega presji czasu (20 proc.). Cieszy fakt, że prawie połowa z nas nie traktuje mediów społecznościowych jako głównego źródła wiedzy, choć tylko 8 proc. sprawdza pochodzenie zdjęć, które widzi przy czytaniu informacji. Jako ochronę przed dezinformacją, 19 proc. Polaków postrzega zgłaszanie i blokowanie treści wątpliwego pochodzenia.

Jest to tym ważniejsze, że informacje dotyczące bankowości np. elektronicznego dostępu do konta czy zasobów gotówki w bankomatach i placówkach bankowych, często bywają zmanipulowane i mają na celu wzbudzenie sensacji, a nawet paniki wśród klientów. Stąd, podstawowa umiejętność tzw. fact checkingu oraz ostrożne podejście do udostępnienia i zwiększania tym samym zasięgów danej informacji, jest dzisiaj bardzo ważnym elementem.

Jakie sposoby Twoim zdaniem są najlepszą ochroną przed skutkami dezinformacji lub fake newsów?

dane w %



źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

3 INCYDENTY I ZAGROŻENIA

INCYDENTY I ZAGROŻENIA

Stosunek do cyberprzestrzeni i stosowanie rozwiązań poprawiających bezpieczeństwo w sieci nie zawsze idą ze sobą w parze. W obliczu ciągłego wzrostu wartości polskiego e-commerce oraz rynku technologii obliczeniowych wysoki poziom wiedzy o cyberprzestrzeni jest na razie jedynie mrzonką. Mimo większej aktywności online w dobie pandemii co drugi Polak według badania „Poziom wiedzy finansowej Polaków 2022" przeprowadzonego na zlecenie WIB i Fundacji GPW wskazuje, że największy niedobór wiedzy odczuwa w obszarze cyberbezpieczeństwa.

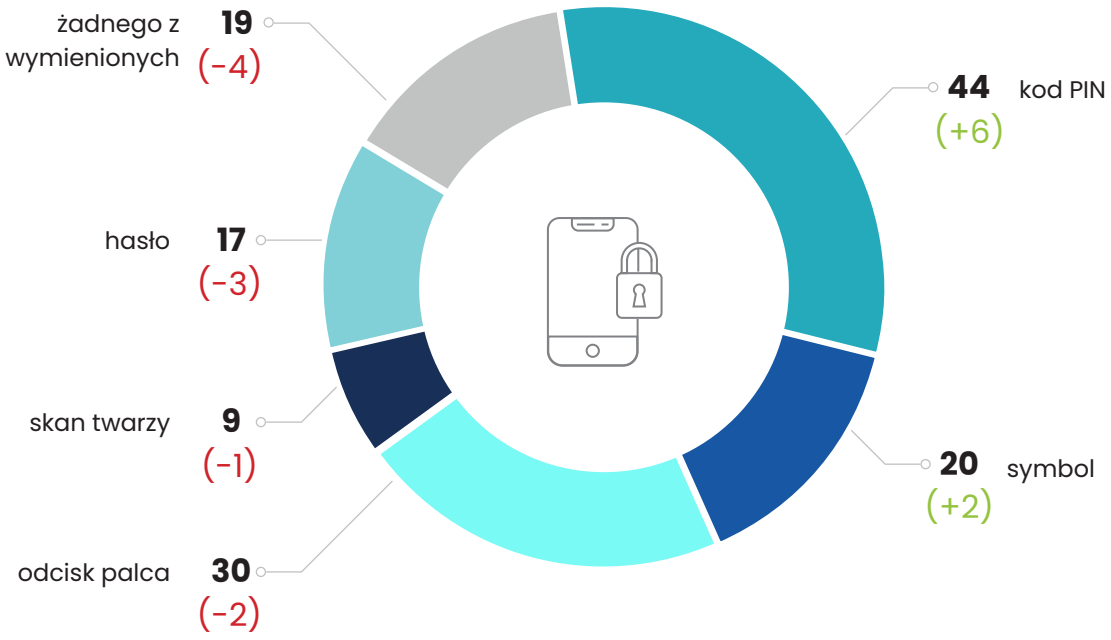
Rozwijanie świadomości cyfrowej na własną rękę jest skuteczne, gdy korzystamy z rzetelnych źródeł informacji. Tymczasem do weryfikowania wiarygodności informacji przyznaje się 16 proc. badanych, 36 proc. robi to często, a sporadycznie 35 proc.

Im mniejsza wiedza, tym bardziej żyzny grunt pod oszustwa. W sieci nie brakuje złych porad, które mogą wykształcić niebezpieczne nawyki. Kryją się za tym często praktyki przestępcze, których celem jest wyłudzenie danych lub środków finansowych.

Jeśli chodzi o podstawowe zabezpieczenia blokady ekranu, Polacy najczęściej stosują kod PIN (44 proc.) lub odcisk palca – tak odpowiedziało 30 proc. badanych. Duży jest także odsetek respondentów, którzy deklarują, że nie używają żadnego zabezpieczenia – 19 proc. Mimo tego, że prawie co piąty z nas nie stosuje zabezpieczeń dostępu do telefonu, ponad połowa deklaruje w badaniach, że posiada zainstalowane aktualne oprogramowanie antywirusowe (52 proc.). Odsetek osób, które odpowiedziały przecząco wyniósł 28 proc, co też wydaje się alarmujące. Zwłaszcza, że nieco ponad 20 proc. nie jest świadoma, czy w posiadanych przez nich urządzeniach zainstalowane jest chroniące przed wirusami oprogramowanie.

Jaki typ zabezpieczenia blokady ekranu/ dostępu do telefonu stosujesz?

dane w % (porównanie rok do roku)

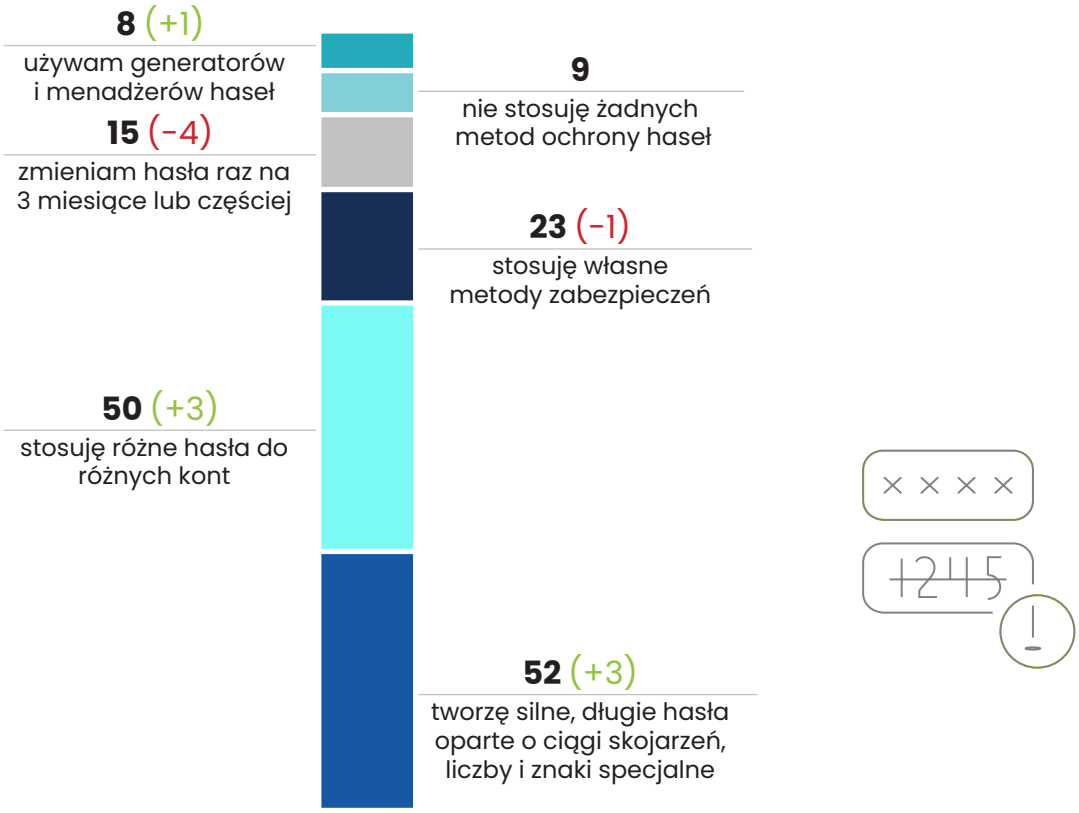


źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Aby chronić swoje dane i hasła co drugi Polak zaznacza w badaniach, że stosuje różne hasła do różnych kont (50 proc.). Wynik w tych granicach osiągnęło także tworzenie silnych i długich haseł, opartych o ciągi skojarzeń– tak deklaruje 52 proc. ankietowanych. Nad zmianą hasła powinniśmy również myśleć dość często. Co 3 miesiące lub częściej robi to 15 proc, a aż 23 proc. deklaruje, że stosuje własne metody zabezpieczeń.

Co robisz żeby zabezpieczać swoje hasła (do np. poczty e-mail, banku, media społecznościowe)?

dane w % (porównanie rok do roku)



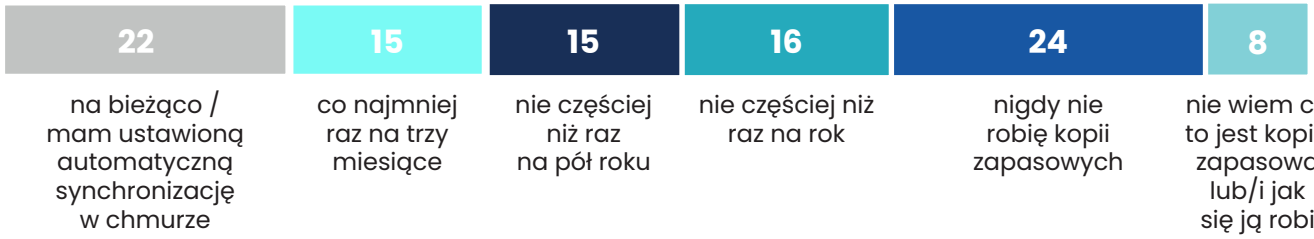
źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Te opinie nie idą w parze ze stosowaniem tych samych haseł do różnych kont np. w banku, poczcie mailowej czy podczas logowania do serwisów społecznościowych. W tym kontekście zdania są podzielone: jedni raczej robią to niechętnie i wykorzystują te same rozwiązania w kilku miejscach, drudzy stosują się do tej reguły dość często. Aż 30 proc. ankietowanych zaznaczyła, że nie stosuje tych samych haseł do różnych kont, rzadko lub bardzo rzadko deklaruje 1/4 ankietowanych. Dla kontrastu, prawie co czwarty Polak stwierdza również w badaniach, że zdarzyło mu się stosować to samo hasło na kilku portalach, a często robiło to 12 proc.

Wielu z nas nie zdaje sobie również sprawy jak istotna jest konieczność wykonywania regularnych kopii zapasowych zgromadzonych danych. Gdy bowiem dojdzie do ataku cyberprzestępców, bez kopii zapasowej, odzyskanie danych z komputera czy smartfona będzie graniczyło z cudem. Warto więc ubezpieczyć się na wypadek zagrożenia. Tymczasem Polacy nie przykładają do tego dużej wagi. Albo mamy ustawioną automatyczną synchronizację w chmurze i wykonujemy ją na bieżąco (22 proc.), albo – jak deklaruje 24 proc. – nigdy nie robiliśmy kopii zapasowych. Odsetek Polaków, którzy regularnie wykonują kopię systemu co najmniej raz na 3 miesiące wyniósł niecałe 15 proc. Nie częściej niż raz na pół roku robi to 15 proc., a raz na rok 16 proc.

Jak często robisz tzw. kopie zapasowe swoich danych zgromadzonych na komputerze lub telefonie?

dane w %

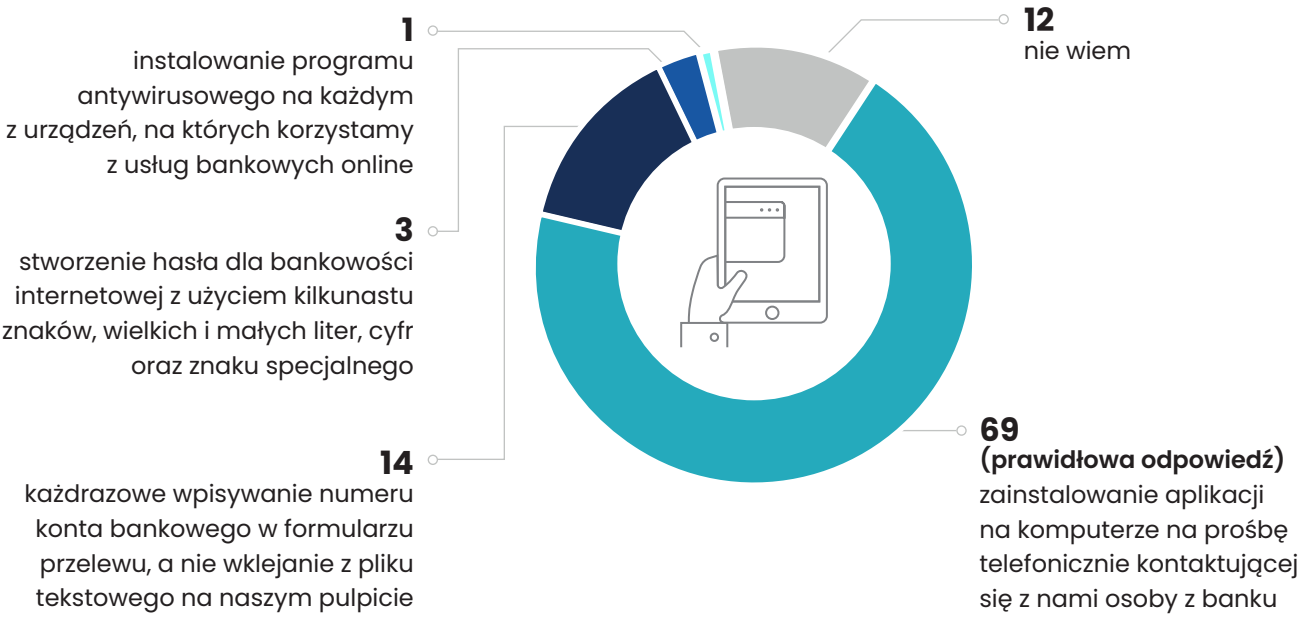


źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Na szczęście konsekwentna edukacja klientów daje nadzieję na stopniowe podnoszenie świadomości w obszarze cyberzagrożeń. Jak wynika z przywołanego już badania „Poziom wiedzy finansowej Polaków" z praktyką zachowań nie jest najgorzej. Blisko 70% badanych umie pośród czterech zachowań w zakresie użytkowania bankowości elektronicznej wskazać niewłaściwą postawą - w tym przypadku jest to zainstalowanie aplikacji na komputerze na prośbę telefonicznie kontaktującej się z nami osoby z banku.

Właściwym zachowaniem w zakresie użytkowania bankowości elektronicznej nie jest:

dane w %



źródło: „Poziom wiedzy finansowej Polaków 2022", CBM Indicator dla WIB i FGPW, 2022.

Pamiętaj prawdziwy pracownik banku nigdy **nie poprosi cię o zainstalowanie** dodatkowego oprogramowania na twoim urządzeniu!

Jeśli otrzymasz taką prośbę telefonicznie lub mailowo **zatrzymaj się!**

Prawdopodobnie jest to **próba oszustwa i uzyskania zdalnego dostępu** do zawartości twojego komputera lub smartfona!

4 WYZWANIA I TRENDY

WYZWANIA I TRENDY

Rozwój nowoczesnych technologii jest obecnie globalny i niezwykle szybki. Wywiera duży wpływ na bezpieczeństwo banków. Celem utrzymania odpowiedniego poziomu bezpieczeństwa, banki muszą chronić swoje zasoby przed cyber atakami, kradzieżą danych, awariami, a jednocześnie zwiększać dostępność danych i aplikacji. To trudne zadanie i wymaga odpowiednich narzędzi, wiedzy i kwalifikacji.

Instytucje finansowe nieustannie mierzą się z przestępstwami finansowymi, a cyberataki z roku na rok stają się coraz bardziej wyrafinowane. Zmniejszenie poziomu ryzyka jest możliwe dzięki cyfrowej transformacji opartej na nowoczesnej chmurze, która oferuje bankom elastyczność i ochronę przed cyberzagrożeniami.

Chmura jako ośrodek zapasowy to model, który jest coraz intensywniej stosowany w bankach, gdyż potencjalnie jest to najprostszy sposób zapewnienia ciągłości dostępu do danych i pracy systemów na wypadek niedostępności centrów przetwarzania danych. Z racji dużej dojrzałości oraz różnorodności rozwiązań dostarczanych przez dostawców chmurowych może to najszybciej umożliwić świadczenie usług IT spoza Polski. Jednak z drugiej strony niesie to też za sobą wiele ryzyk, którymi trzeba należycie zarządzać, oraz wyzwań operacyjnych (zmiana modelu działania) i regulacyjnych. Wydaje się to być właściwym kierunkiem, ponieważ rozbudowa infrastruktury o zabezpieczenia informacji pozwala chronić dane i zasoby, a także ujednolicić działania podejmowane w celu zachowania zgodności z przepisami prawa bankowego. Aby przeciwdziałać coraz większym cyberzagrożeniom i częstszym nadużyciom, branża finansowa potrzebuje opartych na sztucznej inteligencji narzędzi do zarządzania zgodnością z przepisami i wykrywania oszustw, a także globalnego, wielowarstwowego podejścia do cyberbezpieczeństwa, które umożliwiałoby szybką identyfikację i rozwiązywanie problemów w dużej skali.

Sektor bankowy zawsze był liderem we wdrażaniu innowacji technologicznych – i tych przyspieszających wprowadzanie nowych produktów i usług, i tych poprawiających interakcję między klientami a biznesem. Wdrażanie rozwiązań chmurowych do niedawna odbywało się stosunkowo powoli. Proces ten jednak przyspieszyły wiodące światowe instytucje finansowe, które mogą być dla branży źródłem wiedzy na temat skutecznej transformacji technologicznej w całym sektorze.

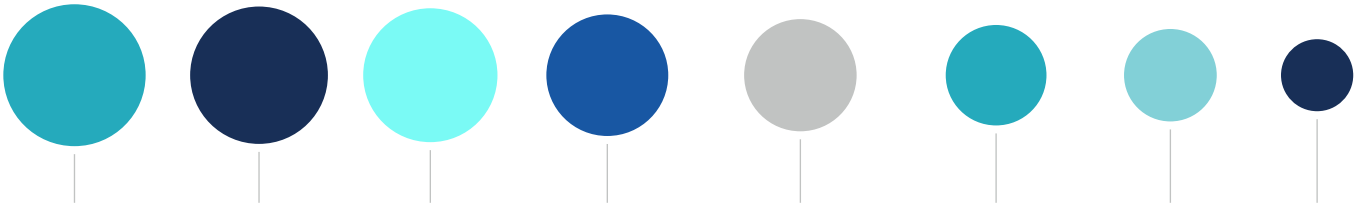
Pod koniec 2021 roku firma GFT przeprowadziła badanie sprawdzające, jak sektor finansowy odbiera technologię chmurową i jak jej wdrożenie pomaga w ulepszeniu procedur i poprawie efektywności w zarządzaniu bankiem. W ankiecie wzięli udział przedstawiciele 21 dużych i średnich banków. Z badania wynika, że 86% banków zaadoptowało usługi w chmurze właśnie po to, aby wykorzystać ich praktycznie nieograniczoną skalowalność.

Coraz większą popularnością cieszą się rozwiązania hybrydowe i wielochmurowe. Większość organizacji rozważa dywersyfikację technologii chmury, a 76% banków uważa, że wdrażanie systemów wielochmurowych od głównych dostawców gwarantuje większe bezpieczeństwo, regularne aktualizacje, nowe usługi i innowacje. Z badań GFT wynika, że optymalizacja kosztów jest głównym powodem, dla którego banki szukają rozwiązań chmurowych w zakresie utrzymania danych. Aż 81% ankietowanych potwierdza, że stosuje technologię chmury właśnie w celu obniżenia kosztów. Badanie GFT wykazało, że 62% bankowców uważa kulturę i pasywność organizacyjną za kluczowe wyzwanie dla sektora finansowego. Innowacje technologiczne usprawniają przeprowadzanie operacji, dzięki czemu stają się one szybsze i bezpieczniejsze.

Zastosowanie chmury zwiększa wydajność organizacji, ponieważ banki wraz ze wzrostem liczby transakcji zużywają mniej zasobów na rozbudowywanie infrastruktury. Zarządzający bankami doceniają tę możliwość – aż 95% z nich rozumie, że technologia chmury może skrócić czas wprowadzania produktów na rynek. Nowe technologie, w tym chmura, budzą także wątpliwości. 43% bankowców przyznało, że to głównie obawy związane z bezpieczeństwem utrudniają im pełną migrację do chmury. Nie ulega jednak wątpliwości, że w przyszłości technologia chmury będzie podstawowym rozwiązaniem dla banków, które chcą rozwijać i skalować swoją działalność, jednocześnie minimalizując ryzyko, czas i koszty. Bankowcy dostrzegają te korzyści, a wyniki przeprowadzonego przez GFT badania sugerują, że inwestycje w technologię chmury będą rosnąć.

Korzyści z chmury dla banków

dane w %



67	63	60	50	43	35	30	19
wydajność operacyjna	skalowalność działalności	szybkość wdrażania innowacji	dostosowanie do rynku	skupienie na zasadniczej działalności	dostęp do ekosystemów	przewidywalność kosztów	bezpieczeństwo

źródło: „Finastra/Obserwator finansowy.pl"

Każdego roku w branży cyberbezpieczeństwa pojawiają się nowe wyzwania, jednak rok 2021 był pod tym względem wyjątkowy. Wzrosła liczba wszelkiego rodzaju ataków, w wyniku których organizacje i firmy na całym świecie musiały stawiać czoła nowym problemom. Zmieniający się świat, w którym żyjemy od chwili wybuchu globalnej pandemii COVID-19 w 2020 roku, okazał się szczególnie sprzyjającym miejscem dla cyberprzestępców. Praca zdalna i postępującą cyfryzacja społeczeństwa, a także przenoszenie kolejnych aspektów naszego życia do Internetu i środowisk cyfrowych oferuje zupełnie nowe możliwości phisherom wykradającym nasze hasła, hakerom, oszustom i internetowym szantażystom.

Analizując najważniejsze wydarzenia nie można nie wspomnieć o największym wyzwaniu 2022 roku czyli wybuchu konfliktu zbrojnego w Ukrainie.

Wybuch wojny wpłynął również na poczucie bezpieczeństwa Polaków w sieci co wskazują podane poniżej wyniki badania. Najwięcej respondentów (41 proc.) wskazała, że umiarkowanie odczuwa obawy związane z tym, że wojna w Ukrainie wpłynie na ich bezpieczeństwo w sieci.

Czy odczuwasz obawy związane z tym, że wojna w Ukrainie wpłynie na Twoje bezpieczeństwo w sieci?

dane w %

źródło: „Postawy Polaków wobec cyberbezpieczeństwa 2022", Pollster dla WIB, 2022.

Wojna w Ukrainie spowodowała przede wszystkim ogromny wzrost liczby cyberataków m.in. na sektor bankowy. W tym też roku dużą aktywność w cyberprzestrzeni można było zauważyć tuż przed wojną. Istotnie zwiększyły się liczby e-maili phisingowych zarówno wymierzonych w stronę pracowników banków jak i skierowanym przeciwko klientom bankowości internetowej w całej Polsce. Wzrosło też tempo tworzenia przez cyberprzestępców fałszywych stron z panelami do wykonywania płatności. Pomimo wyraźnego wzrostu cyberincydentów należy stwierdzić, że sektor bankowy jest bardzo dobrze przygotowany do wykrywania i odpierania cyberataków m.in. dzięki szerokiej współpracy w ramach Bankowego Centrum Cyberbezpieczeństwa. Zarówno Związek Banków Polskich, jak i Urząd Komisji Nadzoru Finansowego koordynują przepływ informacji na ten temat między instytucjami finansowymi. Sektor bankowy coraz bardziej dba o cyberbezpieczeństwo poprzez wykorzystywanie odpowiednich algorytmów, sztucznej inteligencji czy uczenia maszynowego. Jednym z największych wyzwań związanych z cyberbezpieczeństwem są masowe kradzieże danych – dla przykładu tylko w ostatnich tygodniach firma Samsung straciła 190 GB danych swoich klientów i informacji o technologiach, z Microsoftu wykradziono dane 38 mln użytkowników. Ofiarami wycieku danych padły też m.in. Coca-Cola czy T-mobile. Takie sytuacje powodują ogromne straty. Przy czym, o ile wcześniej dominowały kradzieże danych dla okupu (ransomware), o tyle teraz coraz częściej przestępcy po prostu kasują wszystkie dane (ataki typu viper). Jeżeli przedsiębiorstwo jest w stanie odtworzyć je z kopi zapasowych to taki atak utrudnia działalność przedsiębiorstwa tylko pod takim kątem, że potrzeba trochę czasu na prawidłowe wznowienie pracy przesiębiostwa. O wiele trudniejsza jest sytuacja kiedy brakuje backupu.

Dużym utrudnieniem są również cały czas zmieniające się metody cyberprzestępców. Świat wprowadza nowe narzędzia ochrony i przestępcy się do tego dostosowują, wypracowując nowe metody ataków. To widać np. w phishingu – zadaniem e-maila phishingowego jest skłonienie odbiorcy do kliknięcia w link, który z kolei zaprowadzi nas na fałszywą stronę, gdzie wpiszemy swoje dane uwierzytelniające, kierując się bezpośrednio w ręce przestępców.

Dlatego też rozwiąznia chmurowe wydają się być potencjalnie najprostszym sposobem zapewnienia ciągłości danych i pracy systemów na wypadek niedostępności centrów przetwarzania danych posiadanych przez banki. Niosą one jednak za sobą wiele ryzyk bezpieczeństwa, którymi trzeba należycie zarządzać, oraz wyzwań operacyjnych i regulacyjnych. Wydaje się to właściwy kierunek z perspektywy zapewnienia ciągłości działania oraz ochrony interesów klientów. Natomiast, aby było to możliwe, wszyscy muszą wywiązywać się ze swoich zadań – z jednej strony dostawcy usług, a z drugiej ich beneficjenci.

5 ABC CYBER-BEZPIECZEŃSTWA

ABC CYBERBEZPIECZEŃSTWA

Postępująca cyfryzacja dzisiejszego świata stwarza zarówno wiele nowych możliwości, jak i zagrożeń dla naszego bezpieczeństwa w sieci. Bardzo szybki rozwój nowych technologii oraz powszechność internetu sprawiają, że bezpieczeństwo cyfrowe jest ważne jak nigdy dotąd, a surfowanie po nieznanych stronach internetowych, brak aktualnego oprogramowania antywirusowego, udostępnianie swoich wrażliwych danych w Internecie, zbyt proste hasła lub ich całkowity brak - to tylko niektóre z podstawowych błędów, które popełniamy codziennie.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to zbiór działań, technik oraz procesów mających na celu naszą ochronę w sieci przed atakami, uszkodzeniami lub nieautoryzowanymi dostępami, które mogą wyrządzić nam wiele szkód. Dane, zabezpieczające działania mogą opierać się na różnych technologiach, procedurach oraz środkach chroniących systemy, urządzenia itd.

Dowiedz się jak Ty możesz chronić się przed cyberatakami. Zapoznaj się z dziesięcioma zasadami cyberbezpieczeństwa i poczuj się bezpiecznie w sieci.

10 zasad cyberbezpieczeństwa

Chroń swoje dane osobowe!

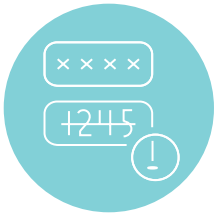
01

Ludzie często świadomie pokazują zbyt wiele w internecie, a czasem po prostu chwalą się np. zdanym prawem jazdy lub nowym dowodem nie znając konsekwencji swoich działań. Dziś oszuści dokładnie wiedzą kogo atakują, a dzięki informacjom, które zostawiasz w sieci oszustwa stają się dużo bardziej wiarygodne, bo złodzieje wiedzą z jakiego banku korzystasz, znają twój pesel, adres lub numer telefonu. Zastanów się dwa razy nad tym co publikujesz w sieci i nie pomagaj cyberprzestępcom.

Aktualny program antywirusowy jest obowiązkiem dla każdego!

02

Nigdy nie wiesz kiedy możesz stać się ofiarą cyberataku. Zabezpiecz swoje urządzenia elektroniczne antywirusem i bądź o krok do przodu przed oszustami. Pamiętaj jednak aby ochrona była skuteczna musisz regularnie aktualizować program. Nie zapomnij o innych urządzeniach po za komputerem. Według najnowszych badań tylko 51% grupy badawczej miało pewność ochrony swojego telefonu. Nie daj się zaskoczyć oszustom, bądź gotowany już dziś.



Zawsze ustawiaj silne hasła!

03

Czy wiesz, że według najnowszych analiz tylko 31 % badanych, na pytanie o stosowanie tych samych haseł do różnych kont (banku, poczty, mediów społecznościowych itd.), odpowiedziało, że nie korzysta z identycznych zabezpieczeń. Tworząc hasło należy pamiętać aby było ono silne, długie i oparte o ciągi skojarzeń, liczby i znaki specjalne. Również pomocne mogą okazać się gotowe generatory oraz tzw. menadżerowie. Takie hasło warto zmieniać co trzy miesiące. Dla stu procentowej pewności można również włączyć m.in. opcję logowania dwuetapowego. Pamiętaj, że jest to pierwszą barierą z jaką musi się spotkać cyberoszust, próbując włamać się na twoje konto. Spraw aby ta ochrona była dla niego nie do przejścia.

Nie zapominaj o wylogowaniu się!

04

Posiadanie silnego, wręcz antywłamaniowego hasła ma sens dopóki będziesz pamiętał o jeszcze jednej sprawie – wylogowaniu! Ta czynność po zakończeniu pracy z danym systemem, aplikacją lub usługą powinno być naturalnym odruchem dla każdego. Jeśli pozostajesz zalogowany dłużej niż potrzebujesz, stwarzasz możliwość nadużycia, włamania czy przejęcia konta. Pamiętaj o wylogowaniu się i w ten prosty sposób zapobiegaj tragedii.

Bądź ostrożny w kwestii bankowości elektronicznej!

05

Aż 70% osób badanych uważa, że banki mają wysokie, jak nie najwyższe, standardy ochrony swoich klientów. To przekonanie stało się świetną przykrywką dla oszustów podszywających się pod instytucje finansowe. Dlatego przede wszystkim należy stosować się do ustalonych zasad bezpieczeństwa zamieszczonych na stronie twojego banku. Jeśli coś odbiega od normy to natychmiast skontaktuj się z obsługą klienta. Pamiętaj, kupując w sklepach internetowych, sprawdzaj czy mają one szyfrowane połączenie – oznaczone kłódką i odpowiednim certyfikatem. Dokonuj płatności tylko z własnego komputera lub telefonu. Dodatkowo, nie wchodź na stronę banku z linku w wyszukiwarce, lecz wpisuj adres ręcznie. Tak samo postępuj z numerem konta odbiorcy naszego przelewu. A jeśli „bank" pyta Cię o hasła, czy też inne poufne dane, np. kod PIN do karty płatniczej, nie odpowiadaj! Na pewno nie jest to bank! Bądź ostrożny!

Nigdy nie odwiedzaj podejrzanych stron!

06

Zanim wejdziesz na nieznaną Ci stronę internetową, upewnij się, że jest ona bezpieczna. Możesz w tym celu użyć wbudowanych narzędzi bezpieczeństwa przeglądarek internetowych, jednak najlepiej zastosuj dodatkowo zewnętrzne narzędzie do sprawdzania witryn. Warto również zweryfikować czy strona posiada certyfikat https. Chodzi o twoje bezpieczeństwo, dlatego pamiętaj - podejrzane strony i linki to także źródło wirusów.

07

Uważaj na wiadomości i linki nieznanego pochodzenia!

Nigdy nie otwieraj wiadomości i dołączonych do nich załączników z nieznanych źródeł. Zawsze weryfikuj linki, które chcesz otworzyć i upewnij się, że wiesz, dokąd one zaprowadzą. Najedź myszką na dowolny link, aby zweryfikować adres URL, z którym jest naprawdę powiązany. Trzeba mieć świadomość, że najczęściej w załącznikach mogą być ukryte złośliwe oprogramowania, wirusy i wiele innych.

08

Zawsze twórz kopię zapasowe!

Tworzenie kopii zapasowej danych, inaczej backup, to nic innego jak dodatkowe zabezpieczenie Twoich plików. Służy ono do odtworzenia oryginalnych danych w przypadku ich utraty bądź uszkodzenia

09

Uważaj na fake newsy!

Uświadom sobie, że klikasz najchętniej w to, co najbardziej lubisz. To sprawia, że widzisz tylko to, co znasz i z czym się zgadzasz. W ten sposób tworzysz wokół siebie tzw. bańkę informacyjną. Pozostając w niej jesteś podatny na fake newsy, które wpływają na nasze emocje, a często nawet na postępowanie. Dlatego cokolwiek czytasz – daj sobie czas na sprawdzenie źródła, autorów, datę publikacji, dokładną analize tekstu i porównanie go z opiniami ekspertów. Cyberprzestępcom chodzi o grę na twoich emocjach i wprowadzenie chaosu lub paniki. Bądź ponad to i nie wierz we wszystko co czytasz w Internecie.

10

Pamiętaj – nigdy nie jest za późno na edukację!

Prawda jest taka, że ludzie nawet nie są świadomi jak wiele jeszcze nie wiedzą! Brakuje im ogólnej edukacji o zagrożeniach w sieci. Dlatego właśnie stają się łatwą ofiarą dla cyberoszustów. Fundacja Warszawski Instytut Bankowości wychodzi temu naprzeciw i edukuje społeczeństwo w tym zakresie od najmłodszych lat, tak aby człowiek był gotowy na czyhające na niego niebezpieczeństwa dzisiejszego świata.

6 PO PIERWSZE EDUKACJA

PO PIERWSZE EDUKACJA

Edukacja zmieniła się na przestrzeni ostatnich lat. Nauczyciele prowadzą coraz więcej zajęć online, a interakcje między studentami, wykładowcami i naukowcami stały się zależne od cyberprzestrzeni.

Zmiany te mają swoich zwolenników jak i przeciwników. Najważniejsze jest jednak to, że sprawiły, iż bezpieczeństwo cybernetyczne i infrastruktura sieciowa znalazły się na celowniku decydentów z zakresu sektora edukacji i nauki. Stało się tak na pewno nie bez powodu ponieważ bezpieczeństwo i łączność stały się niezbędne. Właściwe postawy użytkowników w cyberprzestrzeni stały się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa. Podnoszenie świadomości w tym zakresie jest niezwykle istotne, 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. Zważywszy na fakt, że z bankowości elektronicznej korzysta coraz więcej ludzi, zarówno młodych, jak i osób dorosłych, warto przekazywać a także poszerzać podstawową wiedzę z zakresu bezpiecznego korzystania z nowoczesnych technologii.

Polacy, pomimo coraz większej aktywności w przestrzeni cyfrowej, wciąż nie dysponują dostatecznie dużą wiedzą z obszaru cyberbezpieczeństwa. W świecie wirtualnym poruszają się sprawnie, ale czy świadomie? Świat wirtualny to dynamiczna przestrzeń, która cały czas ewoluuje. Oznacza to, że aby być jej świadomymi użytkownikami, powinniśmy nieustannie się jej uczyć. Badanie „Poziom wiedzy finansowej Polaków 2022", przeprowadzone przez Fundację Warszawski Instytut Bankowości i Fundację Giełdy Papierów Wartościowych wskazuje, że cyberbezpieczeństwo jest tematem „pierwszej potrzeby" wymagającym poprawy, ponieważ ponad połowa Polaków odczuwa brak wiedzy

Kampania „Bankowcy dla CyberEdukacji"

Sektor bankowy w Polsce realizuje wspólną kampanię filmową "Bankowcy dla CyberEdukacji", koordynowaną przez Fundację Warszawski Instytut Bankowości we współpracy ze Związkiem Banków Polskich i ponad dwudziestoma bankami. Dotychczas w ramach pięciu edycji, zrealizowano 120 odcinków edukacyjnych z udziałem blisko 100 ekspertów i znanych osób. W tegorocznej edycji do grona ambasadorów kampanii dołączyli aktorzy: Cezary Pazura i Ewa Kasprzyk.

Celem kampanii, która dotarła już do ponad 2 milionów odbiorców jest edukacja w zakresie zagadnień dotyczących bezpieczeństwa finansów, zakupów online, ochrony tożsamości czy uświadomienia na temat szans i zagrożeń związanych z aktywnością w cyberprzestrzeni. We wspólne działania zaangażowani są eksperci oraz znani i lubiani goście, którzy opowiadają widzom o tym, jak ważne jest bezpieczeństwo w internecie. Tegoroczni ambasadorzy dołączyli do grona takich osób jak m.in. aktor Michał Piela, standuperzy Michał Kempa i Piotr Szumowski, satyrycy Artur Andrus i Grzegorz Halama czy dziennikarze Maciej Orłoś i Beata Tadla, którzy uczestniczyli w poprzednich edycjach kampanii.

„Bankowcy dla CyberEdukacji" to aktualne tematy - oszustwa na rynku Forex, problem fake newsów, ochrona danych osobowych i uwierzytelniających, wyłudzenia na znajomego, czy oszustwa matrymonialne – to niektóre z tematów poruszanych w nowej odsłonie kampanii. Filmy skierowane są do bardzo szerokiej grupy odbiorczej – uczniów szkół podstawowych, szkół średnich, studentów oraz seniorów.

- To bardzo ważne i potrzebne. Kilka lat temu zrobiłem zdjęcie biletu lotniczego i wrzuciłem do mediów społecznościowych. Głupie, ale prawdziwe... Dziś już bym tego nie zrobił – opowiadał na planie filmowym Cezary Pazura. - Mam koleżankę, która online padła ofiarą oszusta matrymonialnego. To się dzieje naprawdę, choć brzmi jak fabuła filmu. – wspominała Ewa Kasprzyk.

Kampania to także nowoczesne sposoby angażowania widzów. „CYFROWO I BEZPIECZNIE. A Ty jak wybierzesz?" to nowatorska forma filmowa, w której widz uczy się przez działanie. Śledzi losy bohaterów i je kreuje, dokonując wyborów. To od widza zależy co wydarzy się dalej. Finałem filmu jest podsumowanie, w którym następuje analiza dokonanych wyborów i wskazanie rozwiązań.

Filmy można zobaczyć tutaj: https://bde.wib.org.pl/multimedia/

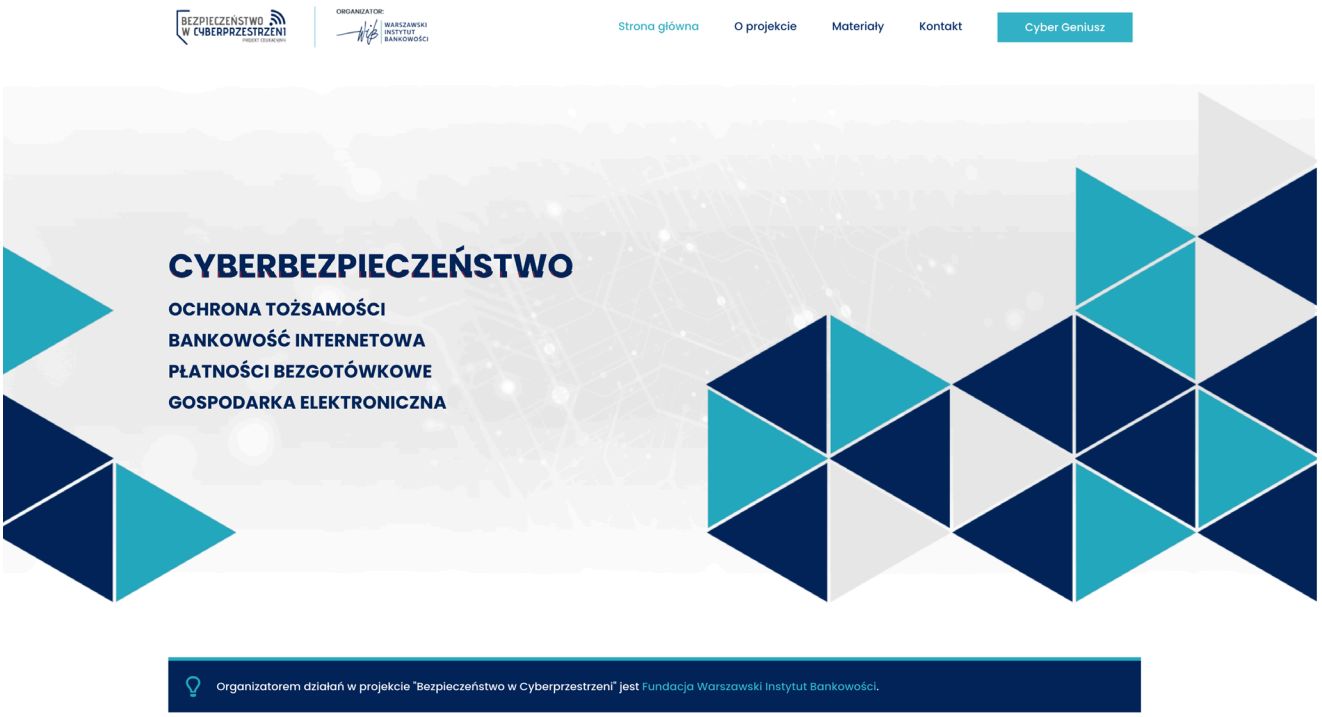
Projekt „Bezpieczeństwo w cyberprzestrzeni”

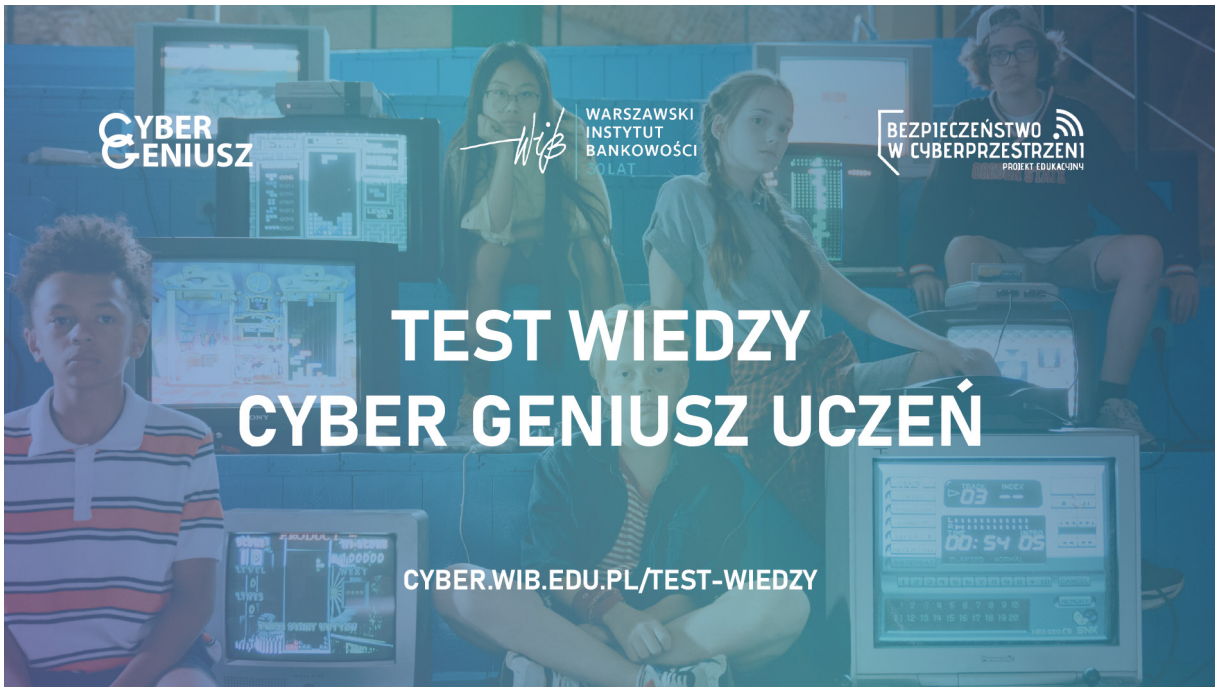
Koordynatorem projektu od 2017 r. jest Fundacja Warszawski Instytut Bankowości, a Partnerami Wspierającymi są Visa, Santander Bank Polska, Fundacja Polska Bezgotówkowa, mBank, Allegro oraz Bank Pekao. Jego celem jest edukowanie Polaków w zakresie umiejętnego i bezpiecznego korzystania z nowoczesnych narzędzi cyfrowych, w tym bankowości elektronicznej, podnoszenie poziomu wiedzy na temat cyberzagrożeń i kształtowanie właściwych postaw w dziedzinie cyberbezpieczeństwa oraz popularyzacja gospodarki elektronicznej.

W ramach projektu realizowanych jest wiele aktywności:

- lekcje i wykłady,
- webinary i szkolenia,
- kursy e-learningowe typu MOOC,
- ogólnopolski test wiedzy Cyber Geniusz,
- sesja tematyczna podczas Kongresu Edukacji Finansowej i Przedsiębiorczości,
- filmy edukacyjne,
- działania medialne,
- raporty, badania i publikacje.

W latach 2017 – 2021 projekt dotarł do ponad 1 mln odbiorców, w tym bezpośrednio do blisko 185 tys. uczniów, 95 tys. studentów i 8 tys. seniorów. Tylko w 2021 roku projekt miał blisko 54 tys. odbiorców, którzy uczestniczyli w ponad 1240 aktywnościach edukacyjnych. Uruchomiona została także nowa strona projektu: www.cyber.wib.edu.pl





Partnerzy wspierający:

allegro mBank POLSKA BEZGOTÓWKOWA Bank Pekao Santander VISA

Jeśli chcesz wiedzieć więcej o bezpiecznym poruszaniu się w sieci lub podejrzewasz, że stałeś się ofiarą cyberataku pomoc znajdziesz tutaj:

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF
https://www.zbp.pl/Dla-Bankow/Cyberbezpieczenstwo

ŹRÓDŁA

Raport realizowany jest w ramach Projektu „Bezpieczeństwo w Cyberprzestrzeni" – jednego z głównych projektów w ramach Programu „Bankowcy dla Edukacji", realizowanego przez WIB.

ZESPÓŁ REDAKCYJNY

Bartłomiej Chlabicz, Julia Dobrzańska, Monika Kondek, Eliza Rokicka

WIĘCEJ INFORMACJI:

FUNDACJA WARSZAWSKI INSTYTUT BANKOWOŚCI

Julia Dobrzańska

512 458 762

jdobrzanska@wib.org.pl

WARSZAWSKI INSTYTUT BANKOWOŚCI 30 LAT

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

BANKOWCY DLA EDUKACJI program sektorowy

ZWIĄZEK BANKÓW POLSKICH