RAPORT ZBP
Cyberbezpieczny portfel

Edycja III

styczeń, 2020 r.

Związek Banków Polskich

Bankowcy dla Edukacji
Program sektorowy

Bezpieczeństwo w cyberprzestrzeni
Projekt edukacyjny

Spis treści

Wprowadzenie

Szanowni Państwo,

dziś, wiele osób nie wyobraża sobie funkcjonowania bez własnych „kluczy" do banku jakimi są karta płatnicza, konto internetowe czy aplikacja mobilna. Przekonaliśmy się o tym na przestrzeni ostatnich kilkunastu lat, w okresie których założonych zostało 37 mln kont z elektronicznym dostępem do rachunku. Jedynie w ciągu ostatnich 12 miesięcy o przeszło 2 mln osób zwiększyła się liczba użytkowników bankowości mobilnej. Aktywność w cyberprzestrzeni to nie tylko wygoda i oszczędność czasu, ale także rosnące wyzwania w obszarze zapewnienia cyberbezpieczeństwa.

Banki w Polsce przeznaczają na ten cel znaczące środki, które w ciągu najbliższych lat będą wzrastać. To nie dziwi, biorąc pod uwagę wnioski płynące z badania przeprowadzonego na zlecenie Związku Banków Polskich w grudniu 2019 r. Wynika z nich, że dla 59 proc. Polaków liderem w zakresie cyberbezpieczeństwa w Polsce są właśnie banki. Warto w tym kontekście zwrócić uwagę na dynamiczny wzrost poziomu zaufania do banków w okresie ostatniego roku aż o 17 p.p. Polacy w zdecydowanej większości czują się bezpiecznie korzystając z nowoczesnej bankowości – aż 90 proc. nie odczuwa niepokoju przy logowaniu się do bankowości internetowej.

Z drugiej jednak strony, mimo że Polacy wskazują na kwestie bezpieczeństwa jako te szczególnie istotne to już praktyczne podejście to tego aspektu nie jest tak powszechne. Jedynie połowa z nas deklaruje, że zmienia hasło do bankowości internetowej co najmniej raz w ciągu 12 miesięcy. Jeszcze mniejsza liczba z nas aktualizuje hasło do bankowości mobilnej – 39 proc. Mimo, że wartości te nie są przesadnie optymistyczne to warto podkreślić, że w porównaniu do danych Komisji Europejskiej, opublikowanych w marcu 2019 r., Polska na tle Europy plasuje się znacznie powyżej średniej. Odsetek mieszkańców Starego Kontynentu odpowiedzialnie podchodzących do kwestii zmiany haseł przy korzystaniu z elektronicznych usług finansowych jest o wiele mniejszy. Takie zachowanie deklaruje jedynie 26 proc. badanych, co jest jednocześnie spadkiem o 3 p.p. w stosunku do poprzedniego pomiaru z 2017 r.

Europejczycy różnią się też jeśli chodzi o stan wiedzy na temat ryzyka związanego z cyberprzestępstwami. W połowie z 28 ankietowanych krajów, większość badanych określiło się co najmniej jako „raczej dobrze poinformowanych". Szczególnie wyróżniają się w tym względzie Duńczycy i Szwedzi (76 proc.), ale odpowiednio wyedukowani czują się także m.in. Brytyjczycy (71 proc.), Holendrzy (69 proc.) i Finowie (67 proc.). Powyżej średniej unijnej (czyli 51 proc., z czego 10 proc. „bardzo dobrze poinformowanych" i 41 proc. „raczej dobrze poinformowanych") plasują się również Polacy z wynikiem 53-procentowym.

Z drugiej jednak strony, aż 40 proc. z nas czuje się słabo lub bardzo słabo poinformowanych w zakresie ryzyk pochodzących z cyberprzestrzeni. Najbardziej alarmujące dane płyną jednak z Rumunii i Bułgarii, gdzie poziom niedoinformowania na ten temat jest największy i wynosi odpowiednio 66 proc. i 65 proc. Co ciekawe niewiele lepiej jest w takich krajach jak Hiszpania (62 proc.), Włochy (59 proc.), czy Belgia (50 proc.).

Analizując te oraz inne dane zawarte w niniejszej, trzeciej edycji raportu „Cyberbezpieczny Portfel", wydawanej we współpracy z Warszawskim Instytutem Bankowości, 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 część poradnikową, która zawiera zbiór zasad podnoszących poziom naszego bezpieczeństwa przy korzystaniu z cyberprzestrzeni, w tym bankowości elektronicznej. Warto się z tym zapoznać i stosować w codziennym życiu.

Związek Banków Polskich

Na początek kilka liczb

1

90%

Polaków czuje się bezpiecznie korzystając z bankowości elektronicznej

Badanie ZBP i CPBiI, grudzień 2019

2

65%

Polaków słabo ocenia swoją wiedzę z zakresu cyberbezpieczeństwa

„Poziom wiedzy finansowej Polaków 2019" Warszawski Instytut Bankowości

3

59%

Polaków postrzega banki jako liderów cyberbezpieczeństwa obok wojska i policji **(40%)** oraz instytucji rządowych **(31%)**

Badanie ZBP i CPBiI, grudzień 2019

4

40%

Polaków deklaruje, że jest słabo poinformowanych na temat ryzyka cyberprzestępstw w sieci

Komisja Europejska, 2019

5

39%

Polaków aktualizuje hasło do bankowości mobilnej minimum raz w roku

Badanie ZBP i CPBiI, grudzień 2019

Polacy wobec bezpieczeństwa w cyberprzestrzeni

Czy czujesz się bezpiecznie korzystając z bankowości elektronicznej?

20% Zdecydowanie **TAK**

70% Raczej **TAK**

7% Raczej NIE

1% Zdecydowanie NIE

2% Nie korzystam z bankowości elektronicznej

Badanie ZBP i CPBiI, grudzień 2019

Korzystając z bankowości w cyberprzestrzeni, Polacy w zdecydowanej większości czują się bezpiecznie. Potwierdzają to wyniki badania na zlecenie Związku Banków Polskich i Centrum Prawa Bankowego i Informacji z grudnia 2019 r. – aż 90 proc. responden-

Odpowiedzialność za bezpieczeństwo finansowych usług elektronicznych ponosi Twoim zdaniem:

81% Bank

30% Klient

20% Instytucje płatnicze (np. MasterCard, Visa)

18% Firma rozliczająca transakcje

11% Operatorzy komórkowi lub internetowi

7% Producent telefonu, komputera, oprogramowania

Badanie ZBP i CPBiI, grudzień 2019

tów uznało, że z bankowością internetową nie wiążą się wyjątkowe niebezpieczeństwa i nie odczuwają większych obaw przy korzystaniu z niej Te dane chociaż mogą cieszyć bankowców, to są jednocześnie źródłem niepokoju. Zbytnia beztroska w korzystaniu z bankowości internetowej i poczucie pełnego bezpieczeństwa może uśpić naszą czujność, co może być brzemienne w skutkach dla naszych pieniędzy. Co ciekawe, znacznie bardziej ograniczone zaufanie do nowoczesnej bankowości mają ci słabiej wykształceni lub zamieszkujący mniejsze miejscowości. Mieszkańcy wsi z wykształceniem podstawowym nie czują się bezpiecznie korzystając z produktów i usług bankowości internetowej w blisko co trzecim przypadku.

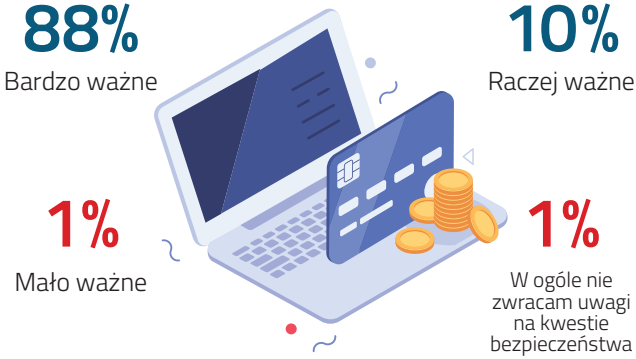
83%
POLAKÓW

oczekuje, że po wystąpieniu cyberataku instytucja niezwłocznie poinformuje ich o jego zajściu i jego skutkach i natychmiast wprowadzi procedury rozwiązujące problem

Związek Banków Polskich, 2018

Jednocześnie, ponad 81 proc. Polaków uważa że podmiotem, który ponosi odpowiedzialność za bezpieczeństwo finansowe usług elektronicznych jest bank. Jedynie niespełna co trzeci ankietowany taką odpowiedzialność przypisał klientowi, a ledwie co piąty instytucji płatniczej. Tymczasem jeśli przeanalizujemy umowy to duża odpowiedzialność jest po stronie klienta który otrzymał od banku narzędzia umożliwiające przeprowadzanie na bieżąco operacji bankowych. Analizując wyniki badania ZBP i CPBiI warto jednak pamiętać, że w przypadku dużej części przestępstw wymierzonych przez hakerów w nasze finanse, odpowiedzialność związana jest ze stosowaniem się do regulaminów i procedur określonych przez banki, w tym ze szczególnym uwzględnieniem przestrzegania poufności danych służących do weryfikacji klienta lub posiadania aktualnego oprogramowania antywirusowego. To szczególnie ważne tym bardziej, że w badaniu zrealizowanym w 2018 roku za najbardziej prawdopodobne zdarzenia z zakresu cyberprzestępczości, sami bankowcy uznali właśnie kradzież danych kart debetowych i kredytowych oraz przechwycenie danych do konta. Warto pamiętać, że w tych obszarach duża część odpowiedzialności spoczywa na kliencie – jest on bowiem we współposiadaniu elementów uwierzytelniających takich jak login, hasło czy karta.

Jak ważne są dla Ciebie kwestie bezpieczeństwa przy korzystaniu z bankowości elektronicznej?



Badanie ZBP i CPBiI, grudzień 2019

Polacy odnoszą się do aspektów bezpieczeństwa związanych z bankowości elektroniczną bardzo odpowiedzialnie chociaż już w kwestii edukacji w tym zakresie nie są tak otwarci na podnoszenie poziomu swojej wiedzy. W dobie nowych programów, aplikacji, a z drugiej strony wirusów i socjotechnik wymierzonych w nasze dane, szczególną rolę powinna odgrywać samodzielna edukacja – i nie chodzi tu o specjalistyczne kursy czy wieloletnie studia. Nie brakuje bowiem wiarygodnych źródeł, z których możemy czerpać artykuły, e-learningi czy filmy i gry edukacyjne. Według niemalże wszystkich respondentów (98 proc. wskazań) bezpieczeństwo w zakresie korzystania z bankowości elektronicznej jest ważne lub bardzo ważne, przy czym w tym drugim wariancie odpowiedzi pozytywnej udzieliło aż 88 proc. ankietowanych. Jednak z perspektywy badania zrealizowanego przez Związek Banków Polskich w 2018 roku, aż 74 proc. respondentów uważało, że nie potrzebuje podnosić swojej wiedzy na temat bezpiecznego korzystania z bankowości internetowej i mobilnej, przy czym w 2019 roku 65 proc. uznało tą wiedzę za niewystarczającą. Biorąc pod uwagę tempo zmian oraz liczbę nowych produktów bankowych, jak również kreatywność cyberprzestępców brak potrzeby edukacji ekonomicznej w tym obszarze generuje istotne ryzyko wśród klientów, jak i samych banków.

65% POLAKÓW
słabo ocenia swoją wiedzę z zakresu cyberbezpieczeństwa

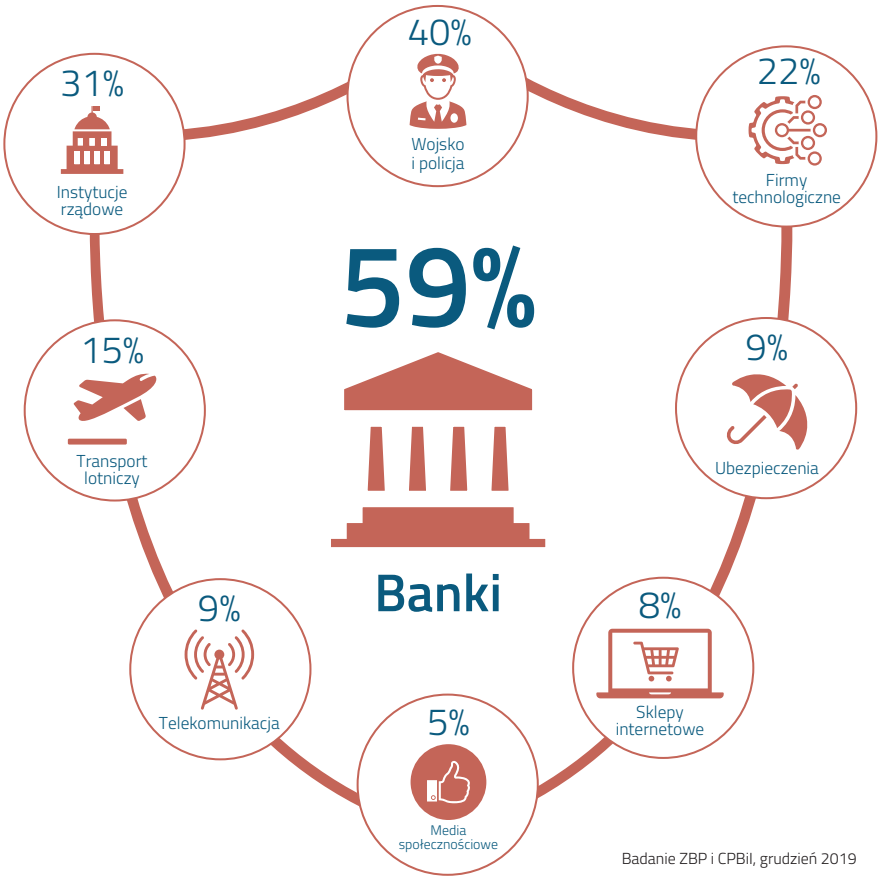
„Poziom wiedzy finansowej Polaków 2019" Warszawski Instytut Bankowości

Bez względu na osobisty stosunek do cyberbezpieczeństwa, Polacy od lat jako branżowego

i instytucjonalnego lidera w tym zakresie postrzegają sektor bankowy - takiego zdania w 2019 r. było 59 proc. ankietowanych. Cieszy nie tylko fakt, że to banki wśród Polaków uznane zostały jako instytucja pierwszego wyboru, ale zwraca również uwagę wzrost poziomu zaufania do instytucji finansowych w okresie ostatniego roku. W ciągu 12 miesięcy poziom wskazań w odniesieniu do banków wzrósł aż o 17 punktów procentowych. Kolejnymi instytucjami, przy istotnie już niższym poziomie zaufania, jest wojsko i policja – 40 proc. (wzrost o 7 p. p.), a co trzeci ankietowany Polak uznał

Zdaniem Polaków banki liderami cyberbezpieczeństwa

Którą z poniższych branż i instytucji postrzega Pan/Pani jako liderów w zakresie cyberbezpieczeństwa?
(możliwość maks. 2 wskazań)



Badanie ZBP i CPBiI, grudzień 2019

90% POLAKÓW

deklaruje, że korzystanie z bankowości internetowej i mobilnej jest bezpieczne.

Badanie ZBP i CPBiI, grudzień 2019

za lidera w obszarze cyberbezpieczeństwa instytucje rządowe (wzrost o 5 p.p.). Wśród instytucji do których Polacy mają ograniczone zaufanie, pozostają sklepy internetowe – jedynie 8 proc. ankietowanych uznało je jako liderów w tym obszarze oraz media społecznościowe 5 proc. wskazań. Równie niepokojąca jest niska ocena w tej kategorii firm ubezpieczeniowych, telekomunikacyjnych, transportu lotniczego czy nawet firm technologicznych.

Deklarowany stosunek do cyberbezpieczeństwa to jedno, a jak wygląda to w praktyce? Polacy, niestety wciąż mają problemy z absolutnymi podstawami w tym zakresie. Jak wynika z badania ZBP i CPBiI jedynie co drugi z nas zmienia co roku hasło do bankowości internetowej. Jeszcze mniejsza liczba respondentów aktualizuje hasło do bankowości mobilnej (39 proc.) Liczbę tę można jednak tłumaczyć mniejszą popularnością bankowości mobilnej w porównaniu do internetowej.

Warto pamiętać że zmiana hasła rzadziej niż raz w roku może generować dodatkowe zagrożenia w wybranych przypadkach. Zazwyczaj częstotliwość zmiany hasła sugeruje nam w swoich komunikatach bank, zawsze możemy o to spytać w placówce, dzwoniąc na infolinię czy poszukać zaleceń na ten temat bezpośrednio na stronach internetowych banku.

Ciągle wielu z nas nie zmienia hasła do banku

Czy w ciągu ostatnich 12 miesięcy zmieniłaś/eś hasło do bankowości internetowej?

49% Tak

38% Nie

11% Nie pamiętam

2% Nie korzystam z bankowości internetowej

Badanie ZBP i CPBiI, grudzień 2019

Czy w ciągu ostatnich 12 miesięcy zmieniłaś/eś hasło do bankowości mobilnej?

39%
Tak

34%
Nie

20%
Nie korzystam z bankowości internetowej

7%
Nie pamiętam

Badanie ZBP i CPBil, grudzień 2019

Niejednokrotnie banki same sugerują potrzebę aktualizacji hasła, należy się wówczas do takich wskazań zastosować aby zwiększyć bezpieczeństwo swoich finansów. Bezwzględnie i niezwłocznie należy jednak hasło zmienić gdy weszły w jego posiadanie osoby trzecie lub nawet w przypadku jedynie stwierdzenia takiego podejrzenia. Warto również pamiętać o odpowiedniej sile hasła oraz stosowaniu ograniczeń i zastrzeżeń rekomendowanych przez bank.

17 proc. Polaków deklaruje, że w ciągu ostatniego roku próbowano od nich wyłudzić prywatne dane. Poziom ten zbieżny jest z analizą Komisji Europejskiej, która wskazuje na taki proceder w przypadku około 16 proc. z nas. Niestety nasze prywatne dane

Czy w ciągu ostatnich 12 miesięcy doświadczyłaś/eś próby uzyskania od Ciebie prywatnych danych za pośrednictwem e-maila lub telefonu?

77%
Nie, nic takiego nie miało miejsca

13%
Tak, zdarzyło się kilka razy

4%
Tak, wiele razy

6%
Nie pamiętam

Badanie ZBP i CPBil, grudzień 2019

14%
POLAKÓW
nie posiada zainstalowanego i aktualnego programu antywirusowego

Warszawski Instytut Bankowości, 2019

21%
POLAKÓW
otwiera załączniki lub klika w linki w mailach od nieznanych nadawców

Związek Banków Polskich, 2018

możemy utracić nieświadomie. Dzieje się tak chociażby w przypadku zainstalowania na naszym komputerze złośliwego oprogramowania, nie mówiąc już o mniej lub bardziej świadomym udostępnianiu tzw. danych wrażliwych. Dlatego tak ważną czynnością okazuje się tworzenie tzw. kopii zapasowych – jednak jak wynika z badania Warszawskiego Instytut Bankowości aż 33 proc. Polaków nigdy nie robi kopii zapasowych swoich danych. Okazuje się także, że w krajach europejskich gdzie świadomość cyberzagrożeń jest większa wzrasta również liczba deklaracji dotyczących prób wyłudzań danych wrażliwych.

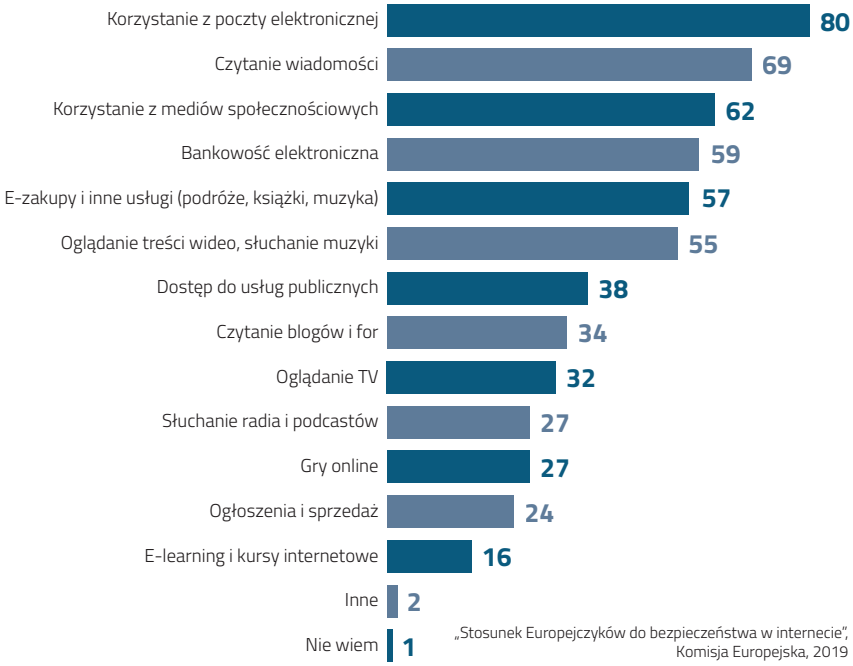
Należy mieć świadomość że kolejne lata przyniosą rozwój przestępczości elektronicznej, a cyberprzestępcy będą poszukiwać kolejnych nisz bazując w dużej mierze na naszej nieświadomości, niewiedzy czy też lekkomyślności. Nie tylko ostrożność, którą chętnie deklarujemy, ale przede wszystkim konsekwentna edukacja i praktycznie rozwijanie posiadanej wiedzy może okazać się najlepszą ochroną przed cyberzagrożeniami.

Poziom wiedzy – Polska na tle Europy

Wraz z rozwojem cyfrowej gospodarki ale i digitalizacją różnych dziedzin naszego życia, nasza aktywność w cyberprzestrzeni jest coraz bardziej zróżnicowana. Potwierdzają to dane Komisji Europejskiej, opublikowane w marcu br. na temat zachowania Europejczyków w kwestii bezpieczeństwa w internecie. Wynika z nich, że najpopularniejszą czynnością w sieci jest korzystanie z poczty elektronicznej, wskazane przez 80 proc. respondentów. Internet jest również źródłem informacji (69 proc.), a także zapewnia dostęp do mediów społecznościowych (62 proc.). Ponad połowa mieszkańców Starego Kontynentu deklaruje, że internet pozwala korzystać im z bankowości elektronicznej (59 proc.), sklepów internetowych i serwisów użytkowych (57 proc.) oraz platform filmowych i muzycznych (55 proc.).

Korzystanie z e-maila wciąż najważniejsze – bankowość w czołówce

Które aktywności online z poniżej wymienionych podejmujesz? (w proc.)

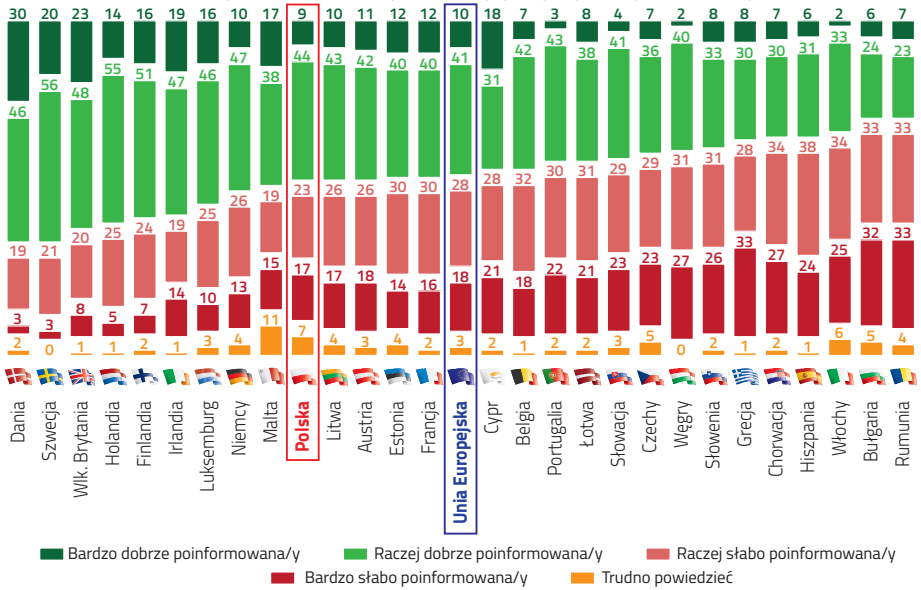


„Stosunek Europejczyków do bezpieczeństwa w internecie", Komisja Europejska, 2019

Tak aktywne korzystanie ze wszystkich możliwości jakie daje cyberprzestrzeń powinno iść w parze, z jednej strony ze świadomością płynących zagrożeń w tym obszarze i pułapek zastawianych na użytkowników, zaś z drugiej z praktyczną wiedzą na temat przeciwdziałania ich potencjalnym skutkom. Tymczasem, jak wynika z danych Komisji Europejskiej, mieszkańcy Europy różnią się jeśli chodzi o stan poinformowania na temat ryzyka związanego z cyberprzestępstwami. W połowie z 28 ankietowanych krajów, większość badanych określiło się co najmniej jako „raczej dobrze poinformowanych". Szczególnie wyróżniają się w tym względzie Duńczycy i Szwedzi (76 proc.), ale odpowiednio wyedukowani czują się także m.in. Brytyjczycy (71 proc.), Holendrzy (69 proc.) i Finowie (67 proc.). Powyżej średniej unijnej (czyli 51 proc., z czego 10 proc. „bardzo dobrze poinformowanych" i 41 proc. „raczej dobrze poinformowanych") plasują się również Polacy z wynikiem 53-proc. Z drugiej jednak strony, aż 40 proc. z nas czuje się słabo lub bardzo słabo poinformowanych w zakresie ryzyk pochodzących z cyberprzestrzeni. Najbardziej alarmujące dane płyną jednak z Rumunii i Bułgarii, gdzie poziom

Świadomość ryzyka w cyberprzestrzeni
Duńczycy na czele, Polacy powyżej średniej unijnej

Jak określasz poziom swojej wiedzy na temat ryzyka cyberprzestępstw w sieci? (proc.)



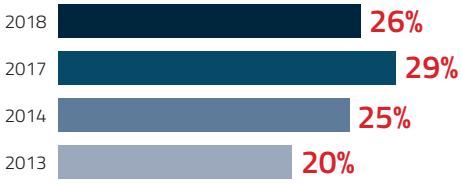
Stosunek Europejczyków do bezpieczeństwa w internecie, Komisja Europejska, 2019

niedoinformowania na ten temat jest największy i wynosi odpowiednio 66 proc. i 65 proc. Co ciekawe niewiele lepiej jest w takich krajach jak Hiszpania (62 proc.), Włochy (59 proc), czy Belgia (50 proc.).

Jedną z niezmiennie ważnych zasad bezpiecznego poruszania się w cyberprzestrzeni jest stosowanie różnych haseł do naszych kont użytkownika i ich zmiana co pewnie okres. Jak pokazuje badanie przeprowadzone na zlecenie Związku Banków Polskich i Centrum Prawa Bankowego, przywoływane w poprzednim rozdziale, Polacy przy korzystaniu z bankowości elektronicznej w większości deklarują, że w ciągu ostatnich 12 miesięcy zastosowali się do tej zasady. Jednak patrząc na analizy Komisji Europejskiej, odsetek mieszkańców Europy odpowiedzialnie podchodzących do kwestii haseł przy korzystaniu z elektronicznych usług finansowych jest o wiele mniejszy. Takie zachowanie deklaruje jedynie 26 proc. badanych, co jest jednocześnie spadkiem o 3 p.p. w stosunku do poprzedniego pomiaru z 2017 r. Oczywiście, należy przy tym pamiętać, że poziom rozwoju i popularności bankowości elektronicznej w Europie jest mocno zróżnicowany, a Polska na tym tle jest jednym z liderów, zarówno pod względem zaproponowanych rozwiązań, jak i kampanii popularyzujących korzystanie z nich.

Jedynie co czwarty Europejczyk pamięta o zmianie hasła do banku

Czy zmieniałaś/eś hasło do bankowości elektronicznej w ciągu ostatniego roku?



„Stosunek Europejczyków do bezpieczeństwa w internecie", Komisja Europejska, 2019

Znacznie lepiej wyglądają dane ogólne, które wskazują, że blisko 6 na 10 użytkowników internetu w Europie zmieniło w ciągu roku swoje hasło do co najmniej jednego z kont użytkownika. Najczęściej dotyczyło to poczty elektronicznej (34 proc. - choć zanotowany przy tym duży spadek w stosunku do poprzednich pomiarów – o 7 p.p. od 2017 r. i aż 11 p.p. od 2015 r.). Na podobnym poziomie jak w przypadku bankowości elektronicznej kształtuje się przekonanie co do zmiany hasła do konta w mediach społecznościowych (24 proc.), natomiast znacznie gorzej wygląda to w odniesieniu do serwisów e-zakupowych (15 proc.).

Łącznie 40 proc. Europejczyków zadeklarowało, że w ciągu roku nie zmieniło żadnego hasła do swoich kont internetowych, co jest niepokojącym wzrostem o 3 p.p. w stosunku do 2017 r., ale jednocześnie wzrostem aż o 10 p.p. od 2015 r.

W Europie częściej zmieniamy hasło do maila niż do konta w banku

Do których z usług elektronicznych zmieniałaś/eś hasło w ciągu ostatniego roku? (w proc.)

„Stosunek Europejczyków do bezpieczeństwa w internecie", Komisja Europejska, 2019

Co drugi Polak ma problemy z podstawową wiedzą finansową

Samoocena stanu wiedzy finansowej Polaków

42% Przeciętna

35% Raczej mała

14% Bardzo mała

7% Raczej duża

2% Bardzo duża

Najsłabiej oceniamy swoją wiedzę z obszarów cyberbezpieczeństwa oraz kredytów i pożyczek

65% Cyberbezpieczeństwo

44% Kredyty i pożyczki

34% Oszczędzanie

34% Finanse publiczne

21% Emerytury

28% Podatki

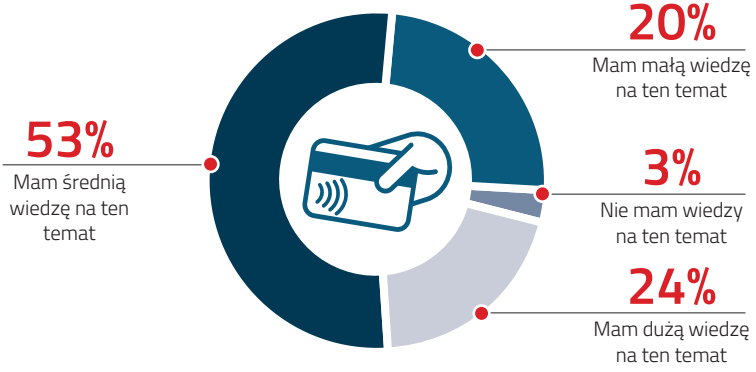
26% Inwestowanie

„Poziom wiedzy finansowej Polaków 2019", Warszawski Instytut Bankowości

Świadomość konieczności zmiany haseł to ważny ale niejedyny aspekt naszego bezpieczeństwa w sieci. Podstawy wiedzy na ten temat są dość obszerne i co ważne wymagają – tak jak programy antywirusowe – stałej aktualizacji. Tymczasem, jak wynika z badań przeprowadzonych w marcu br. na zlecenie Warszawskiego Instytutu Bankowości i Fun-

Nowoczesne płatności (raczej) dość dobrze znane Polakom

Jak oceniasz poziom swojej wiedzy nt. płatności bezgotówkowych, internetowych i pieniędzy elektronicznych?

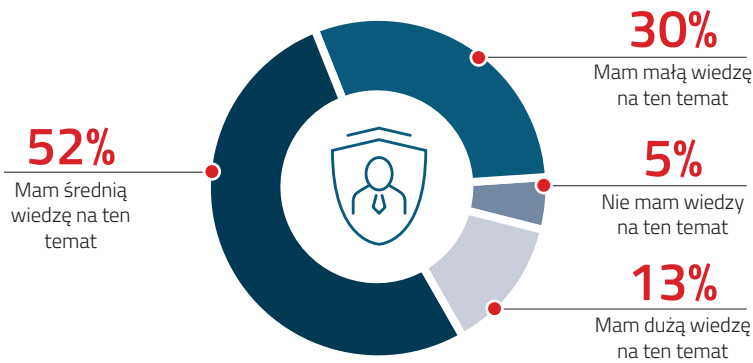


„Wiedza finansowa Polaków", Maison & Partners / Wonga, 2019

dacji Giełdy Papierów Wartościowych, jako Polacy dość krytycznie podchodzimy do swojej wiedzy finansowej. Jedynie 9 proc. Polaków określa ją jako dobrą lub bardzo dobrą. Szczególnie nisko oceniają się młodzi w wieku 18-34 lata (57 proc. wskazań) oraz osoby powyżej 65. roku życia (56 proc. wskazań). Duże problemy ten obszar wiedzy sprawia również mieszkańcom wsi, wśród, których 58 proc. osób nie określa własnego pozio-

Mamy problem z ochroną własnych danych osobowych

Jak oceniasz poziom swojej wiedzy nt. ochrony danych osobowych przed niezbezpieczeństwami w internecie?



„Wiedza finansowa Polaków", Maison & Partners / Wonga, 2019

mu znajomości zagadnień finansowych choćby jako przeciętnego. To co w tym badaniu martwi to fakt, że najsłabiej ankietowani ocenili swoją wiedzę właśnie z zakresu cyberbezpieczeństwa (65 proc.).

Nieco bardziej optymistyczne wnioski płyną z badania „Wiedza finansowa Polaków" Maison & Partners dla Wongi. Wynika, z nich że w obszarze płatności bezgotówkowych i płatności w internecie Polacy są generalnie dość dobrze zorientowani. Blisko 3 na 4 ankietowanych (74 proc.) określa wiedzę na ten temat jako średnią lub dużą.

Bardzo ważnym aspektem przy aktywnym korzystaniu z internetu jest kwestia ochrony danych osobowych. Hakerzy stosują rozmaite sposoby wyłudzenia tzw. danych wrażliwych i umiejętność rozpoznania podejrzanych sytuacji w tym zakresie jest niezwykle istotna. Tutaj wnioski płynące z badania dla Wongi są już mniej optymistyczne. Co trzeci z Polaków deklaruje de facto, że w tym zakresie ma bardzo poważne braki, co w kontekście choćby ataków phishingowych jest bardzo niepokojącą tendencją

Cyberbezpieczeństwo w firmach i przedsiębiorstwach

Aktywność w cyberprzestrzeni nie dotyczy tylko osób indywidualnych, ale również różnej wielkości firmy i przedsiębiorstwa.. Jednak wraz z wprowadzanymi udogodnieniami pojawiają się nowe zagrożenia. Zgodnie z Barometrem Cyberbezpieczeństwa, przygotowanym przez KPMG w kwietniu 2019 roku, aż 70 proc. przedsiębiorstw odnotowało przynajmniej jeden cyberincydent, przy czym 25 proc. firm zauważyło wzrost cyberataków w porównaniu z rokiem 2018. Największym zagrożeniem dla firm okazuje się złośliwe oprogramowanie – szpiegujące lub szyfrujące dane oraz kradzież danych przez pracowników. Problemem jest także brak przeszkolonej kadry (63 proc.), który jest bardziej znaczący niż zbyt mały budżet (61 proc.). Pomimo, że zdecydowana większość przebadanych firm doświadczyła cyberataku to jedynie 57 proc. opracowało procedury na taki wypadek, a co trzecia firma nie planuje inwestować w dalsze zabezpieczenia przed cyberzagrożeniami.

Podobne statystyki wykazują raporty PwC: 22 proc. polskich firm typuje aspekty technologiczne (m. in. cyberbezpieczeństwo) jako potencjalne czynniki, które mogą wywołać kryzys w organizacji. Tylko w 2017 roku w wyniku cyberataków straty finansowe poniosło 44 proc. polskich przedsiębiorstw, a 21 proc. z nich padło ofiarą zaszyfrowania dysku przez złośliwe oprogramowanie. Dodatkowo 20 proc. średnich i dużych firm nie ma ani

Próby ataków hakerskich to już codzienność dla wielu firm w Polsce

Cyberataki pozostają powszechnym zjawiskiem wśród firm prowadzących działalność w Polsce. W 2018 roku przynajmniej jeden cyberincydent odnotowało blisko

70%

ankietowanych przedsiębiorstw.

Wzrost liczby cyberataków w 2018 roku odnotowało **25%** firm. Tymczasem spadek liczby cyberincydentów zauważyło zaledwie **8%** organizacji.

Zaledwie **57%** ankietowanych firm **opracowało procedury reagowania bądź plany zarządzania kryzysowego** na wypadek wystąpienia cyberataku.

„Barometr Cyberbezpieczeństwa – w obronie przed cyberatakami", KPMG, 2019

jednego specjalisty ds. cyberbezpieczeństwa, a budżety przeznaczane na bezpieczeństwo to zaledwie ok. 3 proc. budżetu zespołów IT. Blisko połowa firm nie ma też opracowanych procedur reakcji na incydenty bezpieczeństwa.

Jak wynika z raportu jedynie 8 proc. z badanych firm posiada wysokie kompetencje w zakresie cyberbezpieczeństwa. Autorzy podkreślają, że najbardziej dojrzałe w zakresie cyberbezpieczeństwa firmy pochodzą z branż sektora finansowego, telekomunikacji energetyki oraz produkcji przemysłowej.

Bankowcy dla Edukacji – poradnik

Według badań Warszawskiego Instytutu Bankowości z marca 2019 r. blisko połowa Polaków (49 proc.) deklaruje, że ich wiedza o finansach jest mała lub bardzo mała. Dla 65 proc. badanych najtrudniejszym do przyswojenia tematem jest cyberbezpieczeństwo, a także kredyty i pożyczki, co deklaruje 44 proc.. Jednocześnie, jedną z najbardziej preferowanych form przyswajania wiedzy na ten temat są filmy edukacyjne (53 proc. wskazań). Dlatego też, w ramach Programu „Bankowcy dla Edukacji" od 2017 r., przygotowywane są kolejne cykle ogólnodostępnych materiałów filmowych. Warto się z nimi zapoznać.

Zeskanuj kod i zobacz krótkie filmy edukacyjne na temat cyberbezpieczeństwa

01 BEZPIECZNE KORZYSTANIE Z BANKOMATU

Wypłacając pieniądze stań blisko maszyny i zasłoń swoim ciałem ekran i klawisze, dodatkowo zasłoń też ręką klawiaturę. Jeszcze przed włożeniem karty do bankomatu sprawdź czy wejście na kartę nie posiada żadnych dodatkowych nakładek w postaci np. doklejonej nietypowej listwy z nawierconymi małymi otworami, elementy działające jak magnes, elementy, które można oderwać czy odkleić itd. Zwrócić również uwagę na klawiaturę – nie powinna być wypukła ani zniekształcona. Wpisując PIN nie trzymaj palców wyłącznie na klawiszach, z których składa się Twój kod. Jeśli wygląd lub funkcjonowanie bankomatu wzbudzi Twoje podejrzenia nie wykonuj transakcji.

02 BEZPIECZEŃSTWO KODU PIN

PIN do karty bankowej nie powinien być nigdzie zapisywany, szczególnie na karcie, w portfelu ani w telefonie. Ułóż PIN, który nie będzie oczywisty (jak data Twoich urodzin czy ciąg takich samych cyfr). Nigdy nie podawaj nikomu swojego PINu, ani nie pożyczaj karty. Pamiętaj o zmianie PINu co jakiś czas, np. raz na pół roku. Aby zwiększyć swoje bezpieczeństwo sprawdzaj także wyciąg z konta, w przypadku podejrzanych transakcji zgłoś problem swojemu bankowi.

03 CHROŃMY SWOJĄ TOŻSAMOŚĆ

Powinniśmy mieć świadomość, że nie tylko zagubienie dowodu tożsamości ale również jego czasowa strata może przyczynić się do naszych problemów w przyszłości. Niejednokrotnie przestępcom nie jest potrzebny oryginał dowodu - wystarczy jego ksero lub dane na podstawie których mogą oni wyrobić repliki dokumentu. Nie należy więc pozostawiać dokumentów bez opieki czy też jako zastaw np. w wypożyczalni. Dokumenty lub dane z nich pochodzące mogą posłużyć w wielu sytuacjach, a wyobraźnia i scenariusze działań przestępców w tym zakresie są niezwykle rozwinięte.

Uważajmy także gdzie umieszczamy informacje o nas i jakiego typu są to dane. Przestępcy monitorują portale w poszukiwaniu danych, które są im potrzebne do dokonania przestępstwa. Często też wyłudzają je poprzez np. fałszywe oferty pracy, propozycje pośrednictwa lub podszywając się pod podmioty prowadzący działalność e-commerce.

Przestępcy posiadający nasze dane osobowe mogą przykładowo wyłudzić kredyt na nasze nazwisko czy też wziąć tzw. chwilówkę w firmie pożyczkowej. W innym przypadku skradziona tożsamość może posłużyć do prowadzenia fałszywej działalności biznesowej lub wyłudzenia towaru od innych przedsiębiorców, a także pieniędzy od klientów pod pretekstem wykonania usługi. Przestępcy na nasze nazwisko mogą także wypożyczyć i sprzedać samochód lub podpisać kilka umów z operatorem telekomunikacyjnym dostając w zamian markowe telefony komórkowe.

Problemy związane z wykorzystaniem naszej tożsamości mogą do nas dotrzeć po kilku miesiącach lub nawet latach. Niestety udowodnienie przestępstwa jest niezwykle uciążliwe i długotrwałe. Bardzo ważną czynnością po utraceniu dokumentu tożsamości jest jego zastrzeżenie. Gdy zastrzegasz dowód, zgłaszasz go do Systemu DOKUMENTY ZASTRZEŻONE. W kilka minut informacja dotrze do wszystkich banków w Polsce, Poczty Polskiej oraz operatorów telefonii komórkowej. Twoja tożsamość jest bezpieczna i nikt nie będzie mógł już potwierdzić tożsamości na podstawie Twojego dokumentu. Dla przezornych warto również zastanowić się nad uruchomieniem usługi Alerty BIK, która powiadomi nas o próbach wykorzystania naszej tożsamości do celów kredytowych.

04 STRACIŁEŚ KARTĘ? NIE RYZYKUJ

Skorzystaj z wygodnego systemu do zastrzegania kart. Zadzwoń na numer (+48) 828 828 828, wypowiedz nazwę banku, system połączy Cię z infolinia Twojego banku, odpowiedz na kilka pytań i zastrzeż swoją kartę.

INSTALUJ ROZWAŻNIE PROGRAMY ZE SPRAWDZONYCH ŹRÓDEŁ

Szczególnie narażone są osoby, które pobierają aplikacje z różnych źródeł, nie tylko z oficjalnych sklepów dostawców i pozwalają tym aplikacjom niczym nieuzasadnione nadawanie uprawnień, które nie są niezbędne do prawidłowego korzystania z aplikacji. Takie fałszywe aplikacje są groźne dla danych zgromadzonych na naszym urządzeniu. Zagrożenie stanowić mogą też phishingowe (czyli wyłudzające dane) e-maile oraz wyskakujące reklamy na stronach, w które możesz kliknąć nawet przez przypadek. Aplikacja antywirusowa może pomóc wykryć fałszywe aplikacje i próby wyłudzeń danych. Pomoże także gdy telefon zostanie zgubiony lub skradziony – wiele antywirusów pozwala na zdalne usuwanie danych

ZABLOKUJ EKRAN

Tak jak nie zostawiasz otwartych drzwi do domu, tak nie zostawiaj otwartego dostępu do swojego telefonu lub laptopa. W czasach weryfikacji odciskiem palca, twarzą czy kilkucyfrowym kodem nie warto podawać swoich danych na tacy. Stosuj zabezpieczenia jakie umożliwia Ci Twoje urządzenie.

AKTUALIZUJ SYSTEM I APLIKACJE

Aktualizacje systemu operacyjnego oraz kluczowych aplikacji oprócz dodatkowych funkcji i możliwości zawierają w sobie wiele dodatków poprawiających bezpieczeństwo naszych danych oraz wirtualnego portfela.

Warto również rozdzielić kanały komunikacyjne, tak by autoryzujące wiadomości np. SMS przychodziły na inne urządzenie, niż to przez które logujemy się do banku. Dzięki temu jeżeli nawet malware, czyli złośliwe oprogramowane, zostanie przez nas zainstalowane to i tak atakujący nie uzyska dostępu do naszego konta bankowego, ponieważ albo nie będzie mógł przeczytać haseł albo nie zaloguje się do aplikacji bankowości elektronicznej.

POMYŚL, SPRAWDŹ ZANIM KLIKNIESZ

Większość ataków polega właśnie na wykorzystaniu ludzkiej naiwności. Przestępcy tworzą komunikat motywujący odbiorcę do tego żeby wykonał szybko jakieś działanie. Nikt nie chce stracić dostępu do maili albo mieć zablokowanego konta bankowego. Dlatego klikamy w podany link żeby uchronić się przed taką sytuacją. Nie powinniśmy tego robić bo banki nigdy nie komunikują się z klientami w tych sprawach w taki sposób.

Czy można uchronić się przed takimi kłopotami? Najlepsza rada, to po prostu nie klikać od razu w link, chwilę pomyśleć, zadzwonić do instytucji lub osoby od której potencjalnie otrzymaliśmy e-mail lub smsa, z pytaniem czy rzeczywiście chcą żebyśmy wykonali nietypowe działania.

Na straży bezpieczeństwa sektora bankowego i jego klientów

FinCERT.pl – BCC ZBP, czyli Bankowe Centrum Cyberbezpieczeństwa (BCC) to instytucja, której celem jest zapewnienie sektorowi bankowemu i jego klientom rozwiązań pozwalających na utrzymanie poziomu cyberbezpieczeństwa adekwatnego do ryzyka związanego z oferowanymi w cyberprzestrzeni produktami i usługami bankowymi.

FinCERT.pl – BCC ZBP realizuje swoje cele poprzez:

1) Budowanie wiedzy i świadomości pracowników oraz klientów sektora bankowego;
2) Ustalanie wspólnych i skutecznych zasad postępowania w obszarze ograniczania ryzyka;
3) Realizację zadań zdefiniowanych przez członków w celu osiągnięcia efektu synergii i optymalizacji kosztów przez nich ponoszonych;
4) Współpracę z pozostałymi uczestnikami krajowego systemu cyberbezpieczeństwa

Więcej informacji: **www.zbp.pl/dla-bankow/Cyberbezpieczenstwo**

Projekt edukacyjny – Bezpieczeństwo w Cyberprzestrzeni

W ramach jednego z największych programów edukacji finansowej w Europie – „Bankowcy dla Edukacji" funkcjonuje projekt – **„Bezpieczeństwo w Cyberprzestrzeni"**. Uczestniczą w nim **banki** (ZBP, Pekao S.A., Santander Bank Polska, ING Bank Śląski i mBank), **fundacje** (KIR Cyberium, Polska Bezgotówkowa), **sklepy internetowe** (Allegro), **firmy IT** (IBM Polska, Microsoft), **agenci rozliczeniowi** (eService) oraz **wydawcy kart płatniczych** (Visa).

Prowadzone w ramach projektu aktywności to m.in. lekcje i wykłady z zakresu cyberbezpieczeństwa, konkursy wiedzy, opracowanie i dystrybucja materiałów edukacyjnych jak np. kursy e-learningowe, gra interaktywna czy filmy edukacyjne.

BEZPIECZEŃSTWO W CYBERPRZESTRZENI
PROJEKT EDUKACYJNY

Projekt od 2017 r. dotarł bezpośrednio do ponad
150 000 uczniów, studentów i seniorów.

Więcej informacji: **www.cyberbezpieczenstwo.edu.pl** oraz u koordynatora projektu:

Fundacja Warszawski Instytut Bankowości – **Bartłomiej Majewski**
Kierownik-Koordynator ds. Projektów Edukacyjnych
tel: 696-350-341, mail: bmajewski@wib.org.pl

ZWIĄZEK BANKÓW POLSKICH

Bankowcy dla Edukacji
Program sektorowy

WIĘCEJ INFORMACJI
ZWIĄZEK BANKÓW POLSKICH

dr Przemysław Barbrich
Doktor nauk ekonomicznych,
wykładowca akademicki.
Dyrektor Zespołu Public Relations ZBP.
tel. 660 763 831
przemyslaw.barbrich@zbp.pl

Paweł Minkina
Doradca Zarządu ZBP.
tel: 603 62 62 69
pawel.minkina@zbp.pl

Michał Polak
Dyrektor ds. programów edukacyjnych WIB
tel. 503 624 032
michal.polak@zbp.pl