Tarnobrzeg

(źródło: www.tarnobrzeg.pl)

PROGRAM „BANKOWCY DLA EDUKACJI”

Edukacja Finansowa - współczesna szczepionka na przyszłe kryzysy gospodarcze

Edukacja Finansowa

- współczesna szczepionka na przyszłe kryzysy gospodarcze

Czy edukacja finansowa jest nam potrzebna? Przecież wiemy skąd biorą się pieniądze, potrafimy korzystać z kart płatniczych, mamy konto w banku i elektroniczny dostęp do niego. Wydaje nam się, że nie jesteśmy szczególne rozrzutni i jakoś wystarcza nam pieniędzy na najważniejsze potrzeby. Czy potrzebujemy wiedzieć coś więcej?

Do roku 2008, większość ludzi, ale także instytucji na całym świecie żyła właśnie w takim przekonaniu. Jednak globalny kryzys gospodarczy, pokazał światu, że oprócz wzmocnienia nadzoru nad rynkami finansowymi, konieczna jest także szeroko rozumiana edukacja finansowa, w której udział będą mieli wszyscy uczestnicy rynku: zarówno instytucje publiczne i finansowe, ale także instytucje pozarządowe i samorządy. Musieliśmy nauczyć się znaczenia słowa ryzyko i zrozumieć, że nie można zadłużać się bez końca i jednym kredytem spłacać kolejnego…. Ale czy na pewno wszystko już wiemy? Czy kolejne kryzysy nam nie grożą? Czy potrafimy podejmować właściwe decyzje finansowe i odpowiedzialnie planować swoją przyszłość? Czy odpowiednio zabezpieczamy swoje pieniądze? Czy posiadamy odpowiednią odporność?

Nowe wyzwania

Kryzysy mają to do siebie, że powracają, choć nie zawsze w tej samej formie. Jednak nie tylko one są wyzwaniem. Codziennie podejmujemy istotne decyzje finansowe, choć nie zawsze jesteśmy tego świadomi. Podpisujemy np. umowę z firmą telekomunikacyjną na wysoki abonament, bo akurat jest promocja na najnowszy model smartfona, nie zawsze zastanawiając się, że będzie on obciążał nasz domowy budżet w długiej perspektywie. Inwestujemy pieniądze w fundusz, który obiecuje 10-procentowy zwrot z inwestycji. Czy w sytuacji, gdy w banku oprocentowanie rachunków jest praktycznie zerowe nie powinna zapalić nam się czerwona lampka? Nie myślimy o oszczędzaniu na emeryturę, pomimo, że ciągłe zmiany w systemie emerytalnym oraz niekorzystna demografia nie dają nam szans nie tylko na

emeryturę pod palmami, ale w skrajnej sytuacji także pod własnym dachem. Nie zabezpieczamy także odpowiednio swoich kont bankowych wobec rosnącej liczby ataków cybernetycznych, które podczas pandemii, wyjątkowo nabrały na sile.

Pandemia COVID-19 pokazała nam ponadto, jak kruche są podstawy naszej pewności finansowej. Wiele małych firm musiało zamknąć swoją działalność, wiele osób straciło pracę, a wiele instytucji stało się celem ataków hakerskich, ponieważ przestępcy wykorzystują każdy kryzys, aby żerować na naszej chęci znalezienia łatwych odpowiedzi na trudne pytania, na naszym braku obycia z technologiami cyfrowymi, a także zmęczeniu i stresie.

Czy Polacy znają się na finansach?

Jak wynika z badania *Poziom wiedzy finansowej Polaków 2021*, przeprowadzonego w marcu br. na zlecenie Warszawskiego Instytutu Bankowości (WIB) i Fundacji GPW, w porównaniu do 2020 r., nieznacznie spadł odsetek osób oceniających swoją wiedzę finansową jako „raczej małą" lub „bardzo małą". Niestety, wzrósł za to poziom negatywnej samooceny w tym obszarze wśród młodych Polaków. Jednocześnie, 3 na 4 Polaków oczekuje zdecydowanie przewodniej roli szkoły i nauczycieli w przekazywaniu wiedzy ekonomicznej. Blisko połowa z badanych wskazuje na konieczność wspierania tego procesu ze strony rodziców, mediów, pracowników sektora finansowego i instytucji państwowych. Ostatni rok intensywniejszej aktywności w cyberprzestrzeni umocnił także czołową pozycję wiedzy z obszaru cyberbezpieczeństwa jako tej, która zdaniem Polaków wymaga największego uzupełnienia. Więcej: https://bde.wib.org.pl/polacy-zaczynaja-coraz-uwazniej-czytac-umowy-przed-podpisaniem-i-chca-wiedziec-wiecej-o-inwestowaniu/

Jak wygląda dzisiejsza edukacja finansowa

Edukacja finansowa, rozumiana też szerzej jako edukacja ekonomiczna, cybernetyczna i z zakresu przedsiębiorczości jest nam dziś potrzebna jak nigdy dotąd. Wciąż nie ma wyczekiwanej Narodowej Strategii Edukacji Finansowej, do stworzenia której Polska zobowiązała się jako członek Organizacji Współpracy Gospodarczej i Rozwoju (OECD) w 2012 roku, jednak różnego rodzaju instytucje realizują działania edukacyjne na własną rękę. Znaczną rolę odgrywa tu sektor finansowy, który w Polsce jest inicjatorem największych programów edukacyjnych i przy wsparciu wielu organizacji, ale także samorządów realizuje od kilku lat projekty, które docierają w każdy niemal zakątek Polski.

– W ciągu ostatniego roku większość Polaków zdecydowaną część swojego życia musiała przenieść do sieci. Praca zdalna, bankowość i zakupy online czy edukacja na odległość stały się naszą codziennością. W parze z tak dużą i zróżnicowaną aktywnością muszą iść odpowiednia świadomość i edukacja cyfrowa – swoista

szczepionka na przyszłe kryzysy gospodarcze. Jednocześnie, warto aby w te wszystkie działania edukacyjne – również w obszarze finansów czy zasad funkcjonowania gospodarki – było zaangażowanych jak najwięcej podmiotów i środowisk – zarówno publicznych, prywatnych, jak i pozarządowych. Tylko w ten sposób będziemy w stanie sprostać tym wyzwaniom gospodarczym i cywilizacyjnym, które przed nami w najbliższych latach. Szczególną rolę w tych działaniach odgrywają polskie samorządy, bez zaangażowania których trudno wyobrazić sobie skuteczną edukację w polskich szkołach – powiedział **Prezes Warszawskiego Instytutu Bankowości – Waldemar Zbytek**.

Program Bankowcy dla Edukacji, którego inicjatorem jest Związek Banków Polskich, a organizatorem Fundacja Warszawski Instytut Bankowości, który skierowany jest do dzieci, młodzieży, studentów i seniorów, w ciągu 5 lat osiągnął niespotykany na skalę europejską zasięg. Nie udałoby się to bez wsparcia dziesiątek organizacji i instytucji, które rozumiejąc szczególną rolę edukacji finansowej z punktu widzenia jednostki, ale także ogółu społeczeństwa i interesu narodowego, wsparły projekt czy to finansowo, czy włączając się podmiotowo w różnego rodzaju przedsięwzięcia. Oprócz blisko 200 instytucji rynku finansowego jest to chociażby ponad 7 tys. szkół i uczelni oraz 400 jednostek samorządu terytorialnego, które dzięki aktywnej współpracy umożliwiły dotarcie z edukacją do młodzieży i studentów, ale także seniorów. Niebagatelną rolę odgrywają media, także samorządowe, w których ukazało się blisko 5 tys. publikacji, z czego ponad 1500 trafiło do społeczności lokalnych za pośrednictwem stron urzędów, bibliotek, centrów kultury czy gazetek gminnych. W ciągu 5 lat ponad 1000 wolontariuszy przeszkoliło 2 miliony uczniów, studentów i seniorów oraz 17 tys. nauczycieli, przeprowadzając 81 tysięcy lekcji i wykładów. Z okazji 5-lecia Programu Bankowcy dla Edukacji, podczas Kongresu Edukacji Finansowej i Przedsiębiorczości, przyznane zostały wyróżnienia dla najbardziej aktywnych i zaangażowanych instytucji, wolontariuszy, pracowników naukowych oraz samorządów. Program realizowany jest dzięki dużemu wsparciu parterów generalnych jakimi są Biuro Informacji Kredytowej i Krajowa Izba Rozliczeniowa. Szczególne podziękowania chcielibyśmy skierować na ręce Pana Prezydenta Dariusza Bożka za wspieranie wspólnych działań edukacyjnych na terenie Miasta Tarnobrzeg, gdyż najważniejsze jest edukowanie lokalnie, blisko ludzi.

Czy to dużo? Na pewno tak. Jednak wciąż wiele jest do zrobienia. Edukację musimy traktować jako proces, w którym uczestniczymy na przestrzeni całego naszego życia, ponieważ świat wokół nas nieustannie się zmienia i musimy dostosowywać się do nowych warunków oraz stawiać czoła nowym wyzwaniom i radzić sobie z zagrożeniami. A odpowiednia wiedza ekonomiczna i postawa przedsiębiorcza to przyszły rozwój i bezpieczeństwo finansowe nie tylko obywatela i budżetu Państwa ale również stabilność finansowa dla polskich samorządów, zaspokajających podstawowe potrzeby każdego z nas.

I nikt nie powinien zadawać już pytania: „Czy edukacja finansowa jest potrzebna?”

*

Relacja z tegorocznego Kongresu, podczas którego szeroko omawiane były kwestie związane z edukacją finansową dostępna jest na stronie: www.kef.edu.pl

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na **www.bde.wib.org.pl**

Bądź CYBERBEZPIECZNY 2020!

Odc. 1.
Karta bankowa to także Twoje dane! Bądź CYBERBEZPIECZNY 2020: Odc. 1. Karta bankowa to także Twoje dane! - YouTube
Odc. 2.
Fałszywe strony bankowe - zawsze sprawdzaj pasek adresu! Bądź CYBERBEZPIECZNY 2020: Odc. 2. Fałszywe strony bankowe - zawsze sprawdzaj pasek adresu! - YouTube
Odc. 3.
Nie instaluj aplikacji z nieznanych źródeł! Bądź CYBERBEZPIECZNY 2020: Odc. 3. Nie instaluj aplikacji z nieznanych źródeł! - YouTube
Odc. 4.
SpyWindow, czyli moc socjotechniki Bądź CYBERBEZPIECZNY 2020: Odc. 4. SpyWindow, czyli moc socjotechniki - YouTube
Odc. 5.
Czytaj uważnie na co się zgadzasz! Bądź CYBERBEZPIECZNY 2020: Odc. 5. Czytaj uważnie na co się zgadzasz! - YouTube
Odc. 6.
Internet Rzeczy - zadbaj o bezpieczeństwo! Bądź CYBERBEZPIECZNY 2020: Odc. 6. Internet Rzeczy - zadbaj o bezpieczeństwo! - YouTube

Cyberbezpieczeństwo

Cyberbezpieczeństwo – od czego zacząć?
https://www.youtube.com/watch?v=5rFK5pnLeNs&feature=emb_logo

Przestrzeń cyber, czyli dzień z życia Polaka
https://www.youtube.com/watch?v=A0czE0q7bLw&feature=emb_logo

Nowe technologie przyszłością sektora bankowego
https://www.youtube.com/watch?v=PLjvwu3MEuQ&feature=emb_logo

Nie daj się oszukać

Nie daj się oszukać: Odc. 1 - Oszustwa na BLIKa:
https://www.youtube.com/watch?v=_vEemlZolAQ&feature=emb_logo

Nie daj się oszukać: Odc. 2 - Spam Google Play i wyłudzanie danych logowania do bankowości: https://www.youtube.com/watch?v=OihjXGy4HKY&feature=emb_logo

Nie daj się oszukać: Odc. 3 - Cyberprzestępcy podszywają się pod różne instytucje:
https://www.youtube.com/watch?v=7V5Bv6ZwtFk&feature=emb_logo

Bezpieczeństwo działań w sieci

Odc. 1 - Mylące rozszerzenia plików:
https://www.youtube.com/watch?v=75Xu_K21ORs&feature=emb_logo

Odc. 2 - Aktualizuj system i aplikacje:
https://www.youtube.com/watch?v=NEIQGLHNdDk&feature=emb_logo

Odc. 3 - Bezpieczeństwo poczty elektronicznej:
https://www.youtube.com/watch?v=IetqZVXGDB8&feature=emb_logo

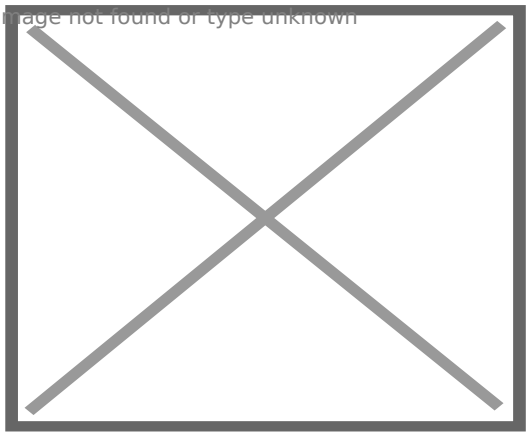
Bądź cyberbezpieczny zawsze

Odc. 1.
Cyberbezpieczeństwo zaczyna się w domu: Bądź cyberbezpieczny zawsze: Odc. 1 - Cyberbezpieczeństwo zaczyna się w domu - YouTube

Odc. 2.
Cyberbezpieczeństwo w miejscu pracy: Bądź cyberbezpieczny zawsze: Odc. 2 - Cyberbezpieczeństwo w miejscu pracy - YouTubeOdc. 3.
Cyberbezpieczeństwo w podróży: Bądź cyberbezpieczny zawsze: Odc. 3 - Cyberbezpieczeństwo w podróży - YouTube

Wirtualna wycieczka po świecie finansów

Image not found or type unknown



WIB zaprasza na "Wirtualną wycieczkę po świecie finansów"

Warszawski Instytut Bankowości zaprasza uczniów i szkoły z całej Polski do skorzystania z możliwości uczestnictwa w wirtualnej wycieczce po świecie finansów. Dzięki niej, bez wychodzenia z domu będzie można poznać najważniejsze instytucje dla sektora bankowego w Polsce. Inicjatywa realizowana w ramach Programu „Bankowcy dla Edukacji" jest jednocześnie jednym z pierwszych elementów działań jubileuszowych związanych z 5. rocznicą uruchomienia Programu, która przypada na 2021 rok.

Ministerstwo Finansów, Narodowy Bank Polski, Bankowy Fundusz Gwarancyjny, Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, Związek Banków Polskich oraz Bank Gospodarstwa Krajowego to instytucje, których historię, zadania i rolę będzie można poznać bliżej dzięki uczestnictwu w inicjatywie WIB.

Ponadto, korzystając z Wirtualnej Wycieczki WIB, będzie można zapoznać się z podstawami nt. finansów, w tym historii pieniądza, domowego budżetu, płatności bezgotówkowych, bankowości internetowej i mobilnej oraz bezpieczeństwa korzystania z usług finansowych.

Na Wirtualną Wycieczkę WIB, w wygodnej formie online można wybrać się bez logowania i bez kupowania biletów. Jej treści wzbogacone są licznymi zdjęciami, animacjami i filmami edukacyjnymi.

Mapa wycieczki: https://bde.wib.org.pl/wirtualna_wycieczka/

Do zobaczenia w świecie finansów!

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego

ze środków Programu Wsparcia Doraźnego Organizacji Pozarządowych w Zakresie Przeciwdziałania COVID-19

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

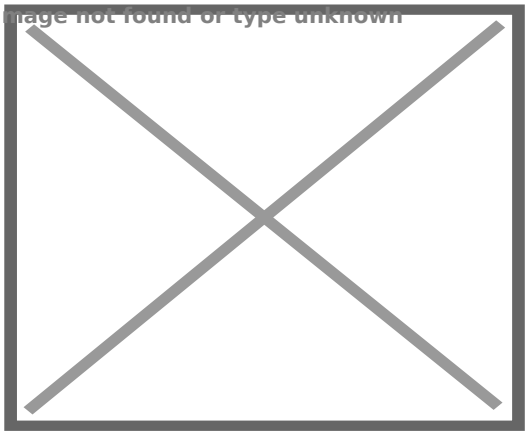
Pliki do pobrania

jpg

Pobierz plik:

bde_-_wirtualna_wycieczka_-_slajd_-_1920x_-_210113_gk2.jpg

Uwaga na złodziei danych osobowych! Przy okazji szczepienia na COVID-19 nie daj się okraść!



Uwaga na złodziei danych osobowych! Przy okazji szczepienia na COVID-19 nie daj się okraść!

W całym kraju ruszył narodowy program szczepień przeciw COVID-19 ogłoszony przez Ministerstwo Zdrowia. To czas, w którym każdy Polak powinien zwrócić szczególną uwagę na bezpieczeństwo swoich danych osobowych. Takie dane jak imię i nazwisko oraz numer PESEL stanowią łakomy kąsek dla złodziei i pierwszy krok do wyłudzenia kredytu czy pożyczki. Jeśli staniesz się ofiarą wyłudzenia danych, możesz uzyskać bezpłatną pomoc w Biurze Informacji Kredytowej.

Uwaga na ujawniony PESEL – niebezpieczeństwo wyłudzenia

Zestaw informacji, składający się z imienia i nazwiska oraz numeru PESEL, to cenna informacja dla potencjalnych złodziei tożsamości. Cenne dane tożsamości znajdują się nie tylko na naszych dokumentach (paszporcie, dowodzie osobistym, prawie jazdy). Są one także w przestrzeni internetowej, w rejestrach, umowach czy dokumentach. O ile o bezpieczeństwo tych pierwszych, możemy dbać sami, tak na pozostałe źródła naszych danych, nie zawsze mamy wpływ. O problemach ze „szczelnością" miejsc przechowywania danych mówią często media, i z nich dowiadujemy się o zagrożeniu kradzieżą lub wyciekiem.

Lista osób do szczepienia – uwaga na kradzież danych

Wiele codziennych aktywności może potencjalnie dawać możliwość pozyskania naszych danych osobowych i wykorzystania ich w celu wyłudzenia kredytu. Są to choćby zakupy w sieci, załatwianie spraw urzędowych, szukanie pracy, czy pobyt na wakacjach.

Masowa akcja, do jakiej należy zaliczyć szczepienie przeciw SARS-CoV-2, także może rodzić zagrożenie bezpieczeństwa naszych danych. Jest to bowiem czas, w którym każdy znajdzie się w sytuacji konieczności potwierdzenia lub przekazania swoich danych tożsamości.

Powszechna akcja szczepień, połączona ze zbieraniem danych osób do zaszczepienia lub już zaszczepionych, wydaje się niestety świetną pożywką dla kampanii phishingowych.

- Prawdopodobnie pojawią się fałszywe e-maile, w których ktoś prosi nas o dane osobowe, rzekomo na potrzeby tworzenia list do szczepienia, podczas gdy tak naprawdę będzie zbierał dane osobowe np. do wyłudzeń finansowych. Zachowujmy zatem baczną uwagę, od kogo dostajemy korespondencję, z rozwagą podawajmy swoje dane, i nie klikajmy pochopnie w linki w wiadomościach e-mail – przestrzega Andrzej Karpiński, szef bezpieczeństwa BIK.

- Osobnym problemem jest zachowanie elementarnej cyberhigieny w zakresie faktycznego tworzenia, gromadzenia, przetwarzania i przesyłania list z osobami do zaszczepienia – takie listy także mogą potencjalnie stać się źródłem wycieku danych osobowych. Udostępniając swoje imię i nazwisko oraz numer PESEL, każdy z nas powinien zadać sobie pytanie, w jaki sposób dany podmiot zadba o nasze dane. Świadomość tego może zaważyć na bezpieczeństwie nas samych. Zwracam uwagę na konieczność zachowania szczególnej ostrożności dziś nas wszystkich, mając na względzie olbrzymią skalę przedsięwzięcia, jaką jest krajowa akcja szczepienia – dodaje Karpiński.

Jeśli nie mamy pewności odnośnie zabezpieczeń danej instytucji

Nasze dane w Internecie, w rejestrach publicznych, na dowodzie osobistym, mogą stać się łupem przestępcy. Gdy trafią w ręce oszustów, mogą posłużyć do zaciągnięcia kredytu lub pożyczki, zawarcia umowy z firmą telekomunikacyjną, wynajmu samochodu i jego kradzieży, założenia firmy na skradzione dane itp. Potencjalne zagrożenie stanowią również wycieki z baz różnych instytucji, wyrzucone dokumenty z danymi klientów.

Co zrobić, jeśli padło się ofiarą przestępstwa?

Jeśli utraciliśmy dokumenty tożsamości, to ważna jest jak najszybsza reakcja. W pierwszej kolejności konieczne jest zastrzeżenie utraconych dokumentów w międzybankowym Systemie Dokumenty Zastrzeżone – można to zrobić w banku lub za pośrednictwem BIK. Kolejnym krokiem powinno być zawiadomienie Policji (jeżeli do utraty doszło na skutek przestępstwa). Warto to zrobić nawet w sytuacji, gdy utraciliśmy dokumenty dawno temu, ale dopiero teraz – z tego artykułu – się Państwo o Systemie DZ dowiedzieli.

Jeśli okazało się, że ktoś na nasze dane (w wyniku np. utraty dokumentów lub wycieku danych w Internecie) wyłudził kredyt lub pożyczkę, po zastrzeżeniu dokumentów i zgłoszeniu sprawy na Policji i tak warto zgłosić się do Biura Informacji Kredytowej.

Na czym polega pomoc BIK dla poszkodowanych?

BIK gwarantuje, że każda osoba, która padła ofiarą wyłudzenia kredytu i ma odpowiednie zaświadczenie z Policji, a zgłosi się do BIK, otrzyma darmowy dostęp do informacji m.in. o tym, w jakich instytucjach finansowych doszło do wyłudzeń, na jaką kwotę opiewają wyłudzone kredyty lub pożyczki oraz czy dany przypadek wyłudzenia jest jedynym, czy doszło do większej liczby nadużyć. Jest to kluczowe dla kolejnych kroków, jakie podejmie pokrzywdzony.

Informacje o wsparciu oferowanym przez BIK poszkodowani w wyniku wyłudzeń kredytów i pożyczek na ich dane znajdą na stronie, https://www.bik.pl/wsparcie

***

Biuro Informacji Kredytowej jest partnerem programu edukacyjnego Nowoczesne Zarządzanie Biznesem, w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym”.

Więcej: www.nzb.pl oraz www.facebook.com/NowoczesneZarzadzanieBiznesem

Antywirus I zaślepka, czyli z czego korzystać, żeby być bezpiecznym w sieci

Programy i narzędzia

Zatrudnij prywatnego ochroniarza do swojego laptopa, czyli zainstaluj program antywirusowy. Zasłaniaj widok przed podglądaczami - stosuj zaślepkę do kamery na urządzeniach. Potwierdzaj w więcej niż jeden sposób, że to Ty, kiedy się gdzieś logujesz za pomocą loginu i hasła. Zgłaszaj się do bliskich i właściwych instytucji, jeżeli natkniesz się na problem w internecie.

Bezpieczeństwo przede wszystkim!

Spotkajmy się w sieci, żeby poznać zasady bezpiecznego korzystania z dóbr technologii, razem.

Zaczynamy?

Film instruktażowy

Jakie wskazówki ma dla nas Barbara Bursztynowicz i jej córka Małgorzata, gdy w grę wchodzi bezpieczeństwo naszych danych? Dlaczego program antywirusowy i uwierzytelnianie dwuskładnikowe to tak przydatne programy, a niepozorna zaślepka do kamerki w laptopie może być tak ważna dla naszej prywatności w sieci?

Zasiądź wygodnie w domowym zaciszu i zobacz film instruktażowy!

https://www.youtube.com/watch?v=f-K4FloHXwk&feature=emb_title

Metody oszustów

Metody oszustów

Seniorze!

Korzystanie z internetu daje nam wiele korzyści, ale podobnie jak w życiu, trzeba uważać na różne zagrożenia. Poznaj powszechne metody oszustów, żeby wiedzieć, na co uważać w sieci oraz aby pamiętać, jak postępować, gdy pojawi się podejrzana sytuacja.

Poczuj się bezpieczniej w sieci, wiedząc na co szczególnie zwracać uwagę.

Film instruktażowy

Czym jest internetowa metoda oszustwa „na wnuczka” i jak się przed nią uchronić? Na czym polega wyłudzenie metodą „na ZUS” i o czym trzeba pamiętać, żeby się jej nie dać? Dowiesz się tego od Barbary Bursztynowicz.

Zobacz film!

https://www.youtube.com/watch?v=eFfC4B2XgAE&feature=emb_title

Karta płatnicza bezpieczniejsza od gotówki

Image not found or type unknown

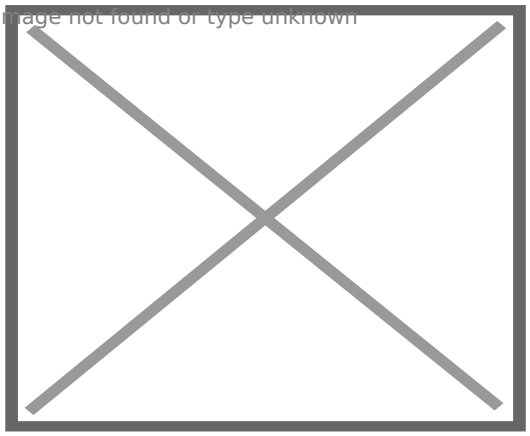


Image not found or type unknown

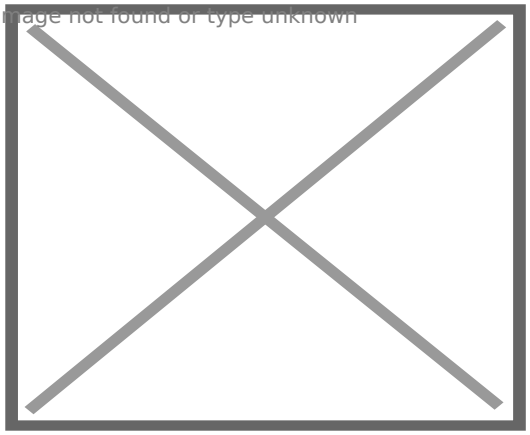


Image not found or type unknown

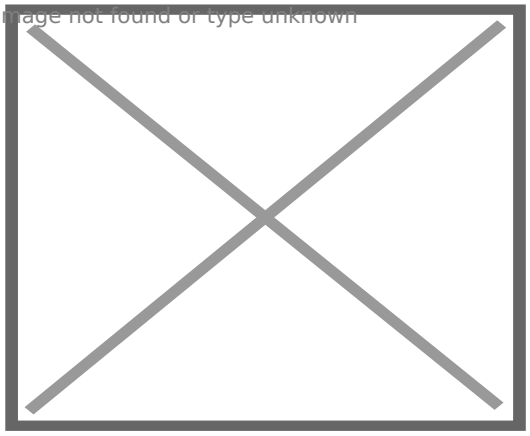


Image not found or type unknown

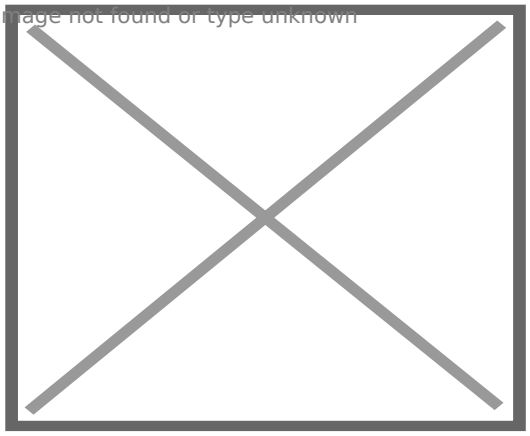
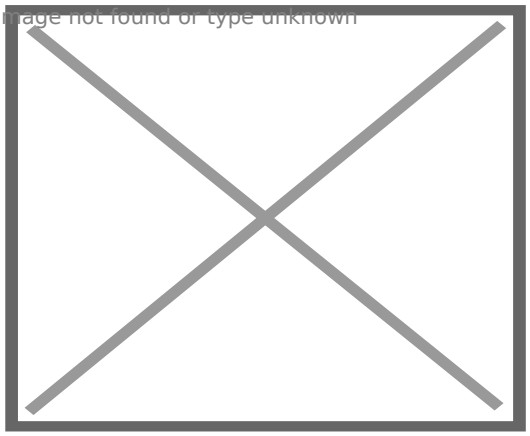


Image not found or type unknown



Karta płatnicza bezpieczniejsza od gotówki

Kiedy zgubimy gotówkę lub ktoś nam ją ukradnie, to na pewno ponosimy stratę finansową. Kiedy z naszego portfela zniknie karta płatnicza, to nie musi to oznaczać straty naszych pieniędzy. Aby kod PIN mógł być skuteczną obroną przed kradzieżą musimy przestrzegać kilku zasad.

Kod PIN możemy znać tylko my. Nie możemy go podawać innej nawet bliskiej osobie. To oznacza, że nie powinniśmy nikomu dawać naszej karty po to, aby wypłacił dla nas pieniądze z bankomatu lub zrobił zakupy.

Kod PIN musimy pamiętać. Nie powinniśmy go nigdzie zapisywać. Jeśli jednak to zrobimy musi być to absolutnie bezpieczne miejsce, a cyfry kodu powinny być tak zapisane, aby nikt postronny nie mógł się domyślić, co one oznaczają.

Przestępca, który będzie miał naszą kartę może jednak próbować złamać nasz kod PIN. Jeśli wybierzemy łatwą do zapamiętania kombinację cyfr np. 1234 lub 1111, albo rok naszego urodzenia to taki PIN nie będzie równie bezpieczny jak kod, do którego wybierzemy przypadkowe cyfry.

Nikt nie powinien zobaczyć, jaki kod PIN wpisujemy na klawiaturze bankomatu, albo na terminalu w sklepie czy w restauracji. Dlatego **kiedy wpisujemy PIN na klawiaturze powinniśmy tę klawiaturę zasłaniać drugą ręką**.

Należy pilnować karty

Aby mieć dostęp do naszych pieniędzy przestępca musi naszą kartę ukraść lub skopiować. Dlatego nigdy nie możemy tracić jej z oczu. W restauracji nie dajemy kelnerowi naszej karty, aby użył jej gdzieś na zapleczu, a stojąc przy ladzie sklepowej nie możemy pozwolić, aby osoba przyjmująca płatność kartą choćby na moment trzymała ją w niewidocznym dla nas miejscu.

Ustaw limity

Transakcje na kwoty poniżej 100 złotych przy użyciu kart, umożliwiają dokonywanie płatności metodą zbliżeniową, czyli bez podawania kodu PIN. Jednak dla naszego bezpieczeństwa można ustawić limity, dzięki którym kolejna próba dokonania transakcji zbliżeniowej na kwotę niższą od 100 złotych będzie jednak wymagała podania kodu PIN.

Stracisz kartę – natychmiast ją zastrzeż

Posiadacz karty z możliwością dokonywania płatności zbliżeniowych, tak jak posiadacz karty płatniczej bez tej możliwości, powinien ją natychmiast zastrzec w momencie, kiedy zorientuje się, że ją zgubił lub mu ją ukradziono. Karty płatnicze można zastrzec w oddziale banku, telefonując na infolinię banku, albo dzwoniąc pod ogólnopolski numer (+48) 828 828 828.

Jeśli potrzebujesz gotówki - skorzystaj z bankomatu, ale pamiętaj:

- Sprawdź czy wejście na kartę nie posiada żadnych dodatkowych nakładek
- Wpisując kod PIN zasłoń klawiaturę ręką
- Wybierz bankomat znajdujący się pod nadzorem kamer, ochrony lub w oddziale banku
- Jeśli cokolwiek wzbudzi Twoje podejrzenia zrezygnuj z transakcji

SZYBKO, WYGODNIE, BEZPIECZNIE – Warto Bezgotówkowo!

RAMKA Warto Bezgotówkowo – Logotyp WB

„Warto Bezgotówkowo” to kampania informacyjna organizowana przez Warszawski Instytut Bankowości we współpracy z Fundacją Polska Bezgotówkowa i Fundacją KIR na rzecz rozwoju cyfryzacji CYBERIUM. Jej celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej płatności bezgotówkowych.

Więcej informacji: WartoBezgotowkowo.pl

Lockdown może uchronić przed COVIDEM, ale nie przed złodziejami tożsamości

Lockdown może uchronić przed COVIDEM, ale nie przed złodziejami tożsamości

Najbliższe tygodnie, a nawet miesiące spędzać będziemy przede wszystkim w domu intensyfikując tym samym naszą obecność w internecie – od zakupów w e-sklepach, aż do znacznie poważniejszych spraw, jak np. szukanie nowej pracy. Tempo cyfryzacji naszego życia, z jakim mamy do

czynienia w ostatnich miesiącach spowodowało, że nie zawsze jesteśmy do tego odpowiednio przygotowani. To stwarza optymalne warunki działania dla zorganizowanych grup przestępczych, pozyskujących dane osobowe w celu prowadzenia kryminalnej działalności.

Wystarczy jeden nieopatrzny ruch, w postaci np. wysyłki online skanu dowodu osobistego lub podania zawartych w nim danych, by zasilić zasoby cybergangów: Pamiętajmy: rzetelny pracodawca nigdy nie wymaga od kandydata do pracy, by ten skanował bądź kserował dowód osobisty!

Takie działania są niezgodne z obowiązującym prawem, poczynając od ogólnego rozporządzenia o ochronie danych (RODO), a kończąc na ustawie o dokumentach publicznych, która wprost penalizuje kserowanie dowodów tożsamości, poza wskazanymi w ustawie wyjątkami. Nie należy do nich z pewnością proces rekrutacji – również w sytuacjach, kiedy odbywa się on w formie zdalnej.

Jeśli zatem w ofercie pracy, lub późniejszej korespondencji z rzekomym pracodawcą, pojawia się warunek wysłania kopii dowodu osobistego, prawa jazdy czy paszportu, można być praktycznie pewnym, iż anons zamieściła grupa przestępcza, a zatem zamiast zatrudnienia mogą czekać nas spore kłopoty.

Podobne problemy oznaczać może skorzystanie z pozornie atrakcyjnej oferty zakupu na raty urządzeń AGD, RTV, sprzętu sportowego czy innych dóbr codziennego użytku, jeśli zamiast zaufanych dostawców tego typu usług, takich jak banki czy renomowane platformy e-commerce, skorzystamy z „super okazji”, to już sama niska cena powinna wzbudzić nasze poważne podejrzenia. Utrata przelanej na konto przestępcy „pierwszej raty” to w takich przypadkach scenariusz… najlepszy z możliwych. Jeśli wysłaliśmy oszustom skan dowodu osobistego, możemy być pewni, iż nie posłużył on do weryfikacji naszej zdolności kredytowej, tylko… no właśnie, do czego?

Kreatywność przestępców jest nieograniczona

Najpewniej do wyłudzenia kredytu w banku lub pożyczki w instytucji pożyczkowej. Dysponując odwzorowaniem dokumentu tożsamości, nawet w formie skanu, sprawcy mogą sporządzić dość wiarygodny falsyfikat, który następnie zostanie przedłożony, jako autentyczny dowód tożsamości rzekomego pożyczkobiorcy.

W przypadku zaciągania zobowiązania w kanałach zdalnych oszust nie musi nawet niczego fałszować, gdyż gros roboty wykonała za niego sama ofiara, fotografując lub skanując dowód osobisty, prawo jazdy lub pierwszą stronę paszportu. Dla przestępcy to znacznie lepsza i bezpieczniejsza opcja aniżeli posłużenie się dokumentem skradzionym w tramwaju bądź sklepie – w tym przypadku bowiem ofiara z reguły jest świadoma popełnionego przestępstwa, istnieje więc duże prawdopodobieństwo, iż o

utracie poinformowała Policję oraz bank.

Pozyskanie odwzorowania dokumentu z reguły nie jest traktowane jako zagrożenie, a wiele osób wręcz nie ma świadomości, że ich dane osobowe znalazły się w niewłaściwych rękach w zupełnie innym celu niż były wysłane oraz jakie mogą być tego konsekwencje. W efekcie o dokonanym oszustwie (lub oszustwach – sprawcy często nie poprzestają na jednorazowym użyciu cudzych danych osobowych!) dowiadujemy się, odbierając nakaz zapłaty lub zawiadomienie o wszczęciu egzekucji komorniczej. Roszczenia w takim przypadku mogą iść w dziesiątki/setki tysięcy, a w skrajnych przypadkach nawet miliony złotych. Udowodnienie, że padliśmy ofiarą cynicznych oszustów jest i żmudne i czasochłonne.

Podobnie może stać się w sytuacji, kiedy sprawcy postanowili z użyciem naszych danych osobowych wyłudzić smartfony, laptopy czy inny sprzęt elektroniczny od operatora telekomunikacyjnego, zawierając umowę – oczywiście bez zamiaru spłaty kolejnych rat zobowiązania.

Kopie dokumentów tożsamości są też wykorzystywane do rezerwacji noclegów, i to nie tylko w hotelach i pensjonatach, ale też w prywatnych mieszkaniach, udostępnianych przez różne serwisy internetowe. W takich przypadkach właściciel nieruchomości, po wyprowadzeniu się najemcy, może zobaczyć gołe ściany, a podejrzenie pada na niewinną osobę, której dane zostały wskazane przy rezerwacji kwatery. W podobny sposób grupy przestępcze kradną samochody, skutery i rowery z wypożyczalni, a nawet są w stanie zarejestrować działalność gospodarczą – np. w celu wyłudzeń podatkowych lub masowych wyłudzeń w e-handlu – wszystko oczywiście bez świadomości osoby, która mimo woli staje się przedsiębiorcą-przestępcą.

Jak skutecznie i bezpiecznie się chronić?

W starciu z dobrze zorganizowanym, a przy tym bezwzględnym przeciwnikiem, jakim są krajowe i międzynarodowe grupy przestępcze i cybergangi, warto wiedzieć, jak skutecznie zapewnić sobie bezpieczeństwo.

Koniecznie – niezwłocznie po uświadomieniu sobie utraty dokumentów, albo też przekazaniu ich skanów w niepowołane ręce – trzeba zgłosić ten fakt do międzybankowego Systemu DOKUMENTY ZASTRZEŻONE. To system wymiany informacji o utraconych dokumentach tożsamości, z którego na bieżąco korzystają banki, instytucje pożyczkowe, operatorzy telekomunikacyjni oraz inni dostawcy usług masowych. Zastrzeżenia możemy dokonać osobiście lub zdalnie – np. poprzez ogólnopolski numer 828 828 828, pod którym możemy także zastrzec utraconą kartę bankową.

W przeciwieństwie do organów ścigania, które odnotowują jedynie utratę dowodu osobistego, paszportu bądź prawa jazdy wskutek popełnienia przestępstwa, w Systemie DOKUMENTY ZASTRZEŻONE uwzględniane są także przypadki zwykłego zagubienia dokumentów.

W sytuacji, kiedy fizycznie nie utraciliśmy dowodu osobistego, paszportu czy innego dokumentu, jednak jego kopię przekazaliśmy osobom trzecim, warto również dokonać zgłoszenia do Systemu DOKUMENTY ZASTRZEŻONE, po czym niezwłocznie wystąpić do właściwego organu o wyrobienie nowego dokumentu.

Jeśli ktoś nie posiada rachunku bankowego, także może udać się do wybranej placówki bankowej, by poinformować o utracie dokumentów! Zgłoszenia zagubienia lub kradzieży przyjmowane są bowiem także od osób niekorzystających z żadnych usług sektora finansowego. Jest to możliwe w wielu bankach komercyjnych i spółdzielczych, których lista znajduje się na stronie www.DokumentyZastrzezone.pl.

Zagrożenie jest poważne: w samym tylko sektorze bankowym, tylko w III kw. br. udaremniono 1.888 prób wyłudzeń kredytów na łączną kwotę 61,3 mln złotych – w całej gospodarce skala przestępczości jest znacznie większa.

Dokonując zgłoszenia utraty dokumentu w banku, nie tylko chronisz się przed negatywnymi skutkami przestępczej działalności z wykorzystaniem Twojej tożsamości, ale w istotny sposób pomagasz tworzyć bezpieczny świat, w którym powody do obaw będą mieli tylko złodzieje i oszuści.

***

Artykuł w ramach Kampanii Informacyjnej Systemu DOKUMENTY ZASTRZEŻONE. Więcej: www.DokumentyZastrzezone.pl

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na **www.bde.wib.org.pl**

Seniorze - spotkajmy się w sieci

Programy i narzędzia

Zatrudnij prywatnego ochroniarza do swojego laptopa, czyli zainstaluj program antywirusowy. Zasłaniaj widok przed podglądaczami - stosuj zaślepkę do kamery na urządzeniach. Potwierdzaj w więcej niż jeden sposób, że to Ty, kiedy się gdzieś logujesz za pomocą loginu i hasła. Zgłaszaj się do bliskich i właściwych instytucji, jeżeli natkniesz się na problem w internecie.

Bezpieczeństwo przede wszystkim!

Spotkajmy się w sieci, żeby poznać zasady bezpiecznego korzystania z dóbr technologii, razem.

Zaczynamy?

Film instruktażowy

Jakie wskazówki ma dla nas Barbara Bursztynowicz i jej córka Małgorzata, gdy w grę wchodzi bezpieczeństwo naszych danych? Dlaczego program antywirusowy i uwierzytelnianie dwuskładnikowe to tak przydatne programy, a niepozorna zaślepka do kamerki w laptopie może być tak ważna dla naszej prywatności w sieci?

Zasiądź wygodnie w domowym zaciszu i zobacz film instruktażowy!

https://www.youtube.com/watch?v=f-K4FloHXwk&feature=emb_title

Metody oszustów

Seniorze!

Korzystanie z internetu daje nam wiele korzyści, ale podobnie jak w życiu, trzeba uważać na różne zagrożenia. Poznaj powszechne metody oszustów, żeby wiedzieć, na co uważać w sieci oraz aby pamiętać, jak postępować, gdy pojawi się podejrzana sytuacja.

Poczuj się bezpieczniej w sieci, wiedząc na co szczególnie zwracać uwagę.

Film instruktażowy

Czym jest internetowa metoda oszustwa „na wnuczka” i jak się przed nią uchronić? Na czym polega wyłudzenie metodą „na ZUS” i o czym trzeba pamiętać, żeby się jej nie dać? Dowiesz się tego od Barbary Bursztynowicz.

Zobacz film!

https://www.youtube.com/watch?v=eFfC4B2XgAE&feature=emb_title

Seniorze – spotkajmy się w sieci

Seniorze – spotkajmy się w sieci!

27 października, 2020

Chcemy pomóc seniorom poznać internet i nauczyć jak bezpiecznie z niego korzystać. To ważne szczególnie teraz, kiedy większość czasu spędzają w domach. Dlatego ruszamy z nową kampanią. Nie jesteśmy sami. Pomaga nam nasza ambasadorka – znana i lubiana aktorka Barbara Bursztynowicz.

„Seniorze – spotkajmy się w sieci” – to hasło kampanii. Realizujemy ją wspólnie z Państwowym Instytutem Badawczym NASK oraz Ministerstwem Cyfryzacji. Partnerami działań WIB są Związek Banków Polskich i Krajowy Instytut Gospodarki Senioralnej – prowadzący platformę interenetową ABC Senior.

Wygrana koncepcja

Jej koncepcja powstała w ramach skierowanego do organizacji pozarządowych konkursu „(Nie)Bezpieczni w sieci”, który ogłoszony został w marcu w ramach kampanii „e-Polak potrafi!”. Laureatem konkursu została Fundacja Warszawski Instytut Bankowości z pomysłem skierowanym do seniorów i kampanią „Seniorze –

spotkajmy się w sieci”.

– Od dłuższego czasu prowadzimy działania zachęcające seniorów do korzystania z internetu. Nowa kampania świetnie się w nie wpisuje. Co więcej, jest potrzebna szczególnie teraz. W czasie, kiedy dla zdrowia i bezpieczeństwa, zachęcamy seniorów do pozostania w domu – mówi Marek Zagórski, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów. – Internet to okno na świat. Ważne, by umiejętnie i bezpiecznie z niego korzystać. Dlatego będziemy tłumaczyć, jak to robić – dodaje minister.

W tym tłumaczeniu pomoże nam ambasadorka kampanii – znana i lubiana aktorka Barbara Bursztynowicz.

– Seniorzy to wyjątkowa grupa społeczna. Z jednej strony z ogromnym doświadczeniem życiowym, a z drugiej coraz aktywniejsza i otwarta na nowe umiejętności. Dziś w obliczu otaczającej nas cyfrowej rzeczywistości, jest niezwykle ważne, aby przestrzeń wirtualna była dla seniorów miejscem jak najbardziej przyjaznym i bezpiecznym – zauważa Michał Polak, wiceprezes Fundacji Warszawski Instytut Bankowości. – Dlatego też chcemy, aby nasza kampania była istotnym krokiem w tym kierunku. Dzięki niej dotrzemy do dziadków, rodziców ale także wnuków i dzieci. Jesteśmy przekonani, że międzypokoleniowa wymiana doświadczeń i wiedzy zwiększy poziom bezpieczeństwa naszych seniorów w cyberprzestrzeni. Pozwoli także pielęgnować relacje, na które mamy coraz mniej czasu – dodaje.

Bezpieczny cel

Współpraca międzypokoleniowa to nasz cel. Dlatego działania kierujemy nie tylko do seniorów, ale i ich bliskich – dzieci i wnuków. Przygotowane zostały proste, napisane przystępnym językiem broszury, ale i krótkie filmy instruktażowe. Filmów będzie pięć, tyle samo broszur. Główną bohaterką filmów jest oczywiście nasza ambasadorka Barbara Bursztynowicz.

Tematy filmów i broszur dobraliśmy tak, aby najpierw pomóc seniorom poznać możliwe zagrożenia w sieci, a później nauczyć ich jak tych zagrożeń unikać. Dlatego pierwsze trzy tematy to: bezpieczne korzystanie w sieci z rozrywki i komunikacji oraz bezpieczne załatwianie online różnych spraw, w tym urzędowych. Kolejne dwa tematy dotyczą sposobów na zabezpieczenie swoich danych w sieci, a także unikania konkretnych metod oszustów w internecie.

Filmy wprowadzają do tematyki każdego z poszczególnych zagadnień, a broszury rozwijają i uzupełniają każdy z nich. Dzięki takiemu ujęciu, senior będzie mógł rozpoznać zagrożenie, ale też dowie się, jak sobie z nim poradzić – sam lub przy wsparciu bliskich – dzieci czy wnuków.

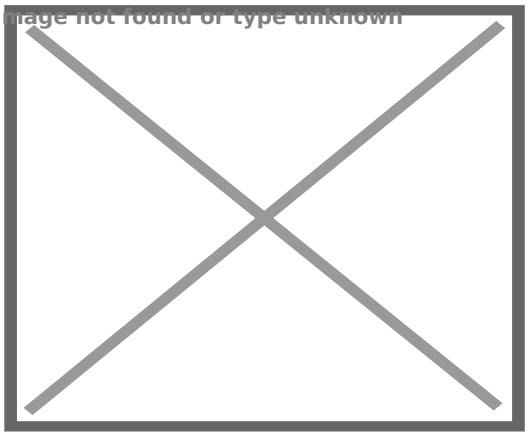
Spektakl i film, czyli o bezpiecznej rozrywce w internecie

E-mail i media społecznościowe, czyli o bezpiecznej komunikacji w internecie

Sprawy urzędowe i bankowe, czyli o bezpiecznym załatwianiu codziennych spraw przez internet

LOGO

Image not found or type unknown



LOGO

Seniorze, nie daj się!

Wyłudzanie pieniędzy od osób starszych poprzez zastraszanie, udawanie policjanta, urzędnika czy członka rodziny niestety wciąż zbiera żniwa – tylko w Warszawie, w ciągu pierwszego kwartału 2018 roku wyłudzono od seniorów ponad 4,3 miliona złotych. W roku 2017 prawie 19 milionów złotych! Policjanci, strażnicy miejscy oraz bankowcy łączą siły w nowej kampanii społecznej, która obejmuje zarówno działania informacyjne, jak i operacyjne.

Metody naciągania osób starszych bazują najczęściej na zaufaniu. Oszuści, podając się za policję, rodzinę, pracowników ZUS-u, opieki społecznej czy fundacji, bez problemu wchodzą do domu, swoją wizytę tłumacząc koniecznością pobrania zaległej opłaty, albo przeciwnie – przekazania jakichś pieniędzy, bądź zachęcają do wsparcia zbiórki na szczytny cel. Ofiara nieświadomie wskazuje miejsce przechowywania gotówki, a sprawca kradnie oszczędności i inne cenne przedmioty, znajdujące się w mieszkaniu. Podczas rozmowy telefonicznej seniorzy namawiani są na przekazanie komuś albo pozostawienie w jakimś miejscu gotówki lub kosztowności. Często skłania się ich do wypłat oszczędności z banku, a nawet do zaciągania kredytów.

Najważniejsze to zachować zdrowy rozsądek!

1. Bądź ostrożny, czujny i przewidujący.
2. Policja nigdy nie prosi o przekazywanie pieniędzy lub kosztowności obcym osobom

ani policjantom.
3. Jeżeli ktokolwiek telefonicznie prosi o pieniądze i masz jakiekolwiek wątpliwości z kim rozmawiasz skontaktuj się z najbliższymi lub policją dzwoniąc pod numer 112.
4. Gdy obce osoby osobiście pojawią się w twoim mieszkaniu - bądź wyjątkowo ostrożny.

Na stronie internetowej www.SeniorzeNieDajSie.pl można znaleźć informacje jakimi metodami posługują się przestępcy i jak reagować w przypadku próby wyłudzenia:

- **Na wnuczka:** dzwoniący podaje się za rodzinę lub przyjaciela rodziny i prosi o pomoc finansową w związku z wypadkiem, chorobą albo wyjątkową okazją do zarobienia pieniędzy. Sytuacja według dzwoniącego jest nagła i wymaga natychmiastowej reakcji ze strony seniora. Dodatkowo dzwoniący twierdzi, że cała sprawa musi pozostać tajemnicą.
- **Na policjanta:** dzwoni policjant i informuję, że grupa przestępcza chce ofiarę okraść – np. ze środków finansowych lub lokat w banku i prosi o współpracę.
- **Na zaliczkę, przedpłatę czy nadpłatę:** nakłanianie do przesłania pieniędzy z góry za jakiś produkt lub usługę lub przekazanie czeku na kwotę wyższą niż ustalona cena, z prośbą o odesłanie nadwyżki środków za pośrednictwem przekazu pieniężnego - czek okazuje się fałszywy.
- **Na ofertę pracy:** prośba o przesłanie pieniędzy w zamian za przyjętą propozycję zatrudnienia.
- **Na loterię, nagrodę:** zawiadomienie o wygranej na loterii i prośba o wysłanie pieniędzy, aby móc odebrać nagrodę.
- **Na nieruchomość:** oferta wynajmu/zakupu nieruchomości i prośba o wysłanie pieniędzy, podając przyczyny, które wydają się wiarygodne, jednak nieruchomość nie jest prawdziwa.
- **Na zakupy przez internet:** prośba o przesłanie pieniędzy w celu zapłaty za produkt, przedmiot aukcji lub usługę reklamowaną w internecie.
- **Na znajomości:** ofiara poznaje kogoś przez internet, nabiera zaufania do tej osoby, a następnie jest proszona o przysłanie pieniędzy.
- **Na chwilówkę:** propozycja unikalnej promocji uzyskania pożyczki, potem okazuje się, że faktyczne oprocentowanie jest bardzo wysokie.
- **Na pracownika administracji, hydraulika, pracownika socjalnego:** pod pretekstem wywiadu środowiskowego, sprawdzenia stanu technicznego instalacji w mieszkaniu, wykorzystując chwile nieuwagi, dokonywane są kradzieże pieniędzy lub kluczy do mieszkania.
- **Na dostawcę prądu / usług telekomunikacyjnych:** w ramach fałszywej promocji podkładane są umowy z zawyżonymi stawkami z inną firmą.

SENIORZE PAMIĘTAJ! ZAWSZE BĄDŹ UWAŻNY, OSTROŻNY I PRZEWIDUJĄCY!

- **Nie izoluj się** – nie trać więzi z rodziną i przyjaciółmi.
- **Szukaj informacji** (internet, prasa, radio, telewizja, instytucje gromadzące i przetwarzające informacje).

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

10 zasad cyberbezpieczeństwa

Zdalny dostęp do własnych pieniędzy przez komputer lub telefon to z jednej strony wygoda, a z drugiej ryzyko, że padniemy ofiarą cyberprzestępców. W raporcie **Polska i Europa. Wyzwania i ograniczenia,** eksperci Związku Banków Polskich zauważają: *Codziennie, na całym świecie atakowanych jest 0,5 mln stron internetowych, a 76 procent stron internetowych ma słabe punkty, przez które można było je zaatakować.*

Czego nie robimy w sieci, a powinniśmy?

Niestety, jak wynika z analiz Komisji Europejskiej – jesteśmy najmniej ostrożnym narodem w UE, jeśli chodzi o zachowania w Internecie. Aż 57 proc. z nas nie instaluje oprogramowania antywirusowego, 72 proc. odwiedza strony internetowe mimo braku przekonania o ich bezpieczeństwie, 83 proc. Polaków używa tego samego hasła do różnych kont, 86 proc. nie zmienia regularnie haseł do posiadanych kont i 92 proc. nie zmienia ustawień dotyczących bezpieczeństwa w przeglądarkach internetowych.

Jeżeli więc chcemy być bezpieczni w sieci, to powinniśmy robić to, czego większość Polaków nie robi.

10 zasad cyberbezpieczeństwa

1. Instalujmy na swoim komputerze dobry program antywirusowy i regularnie go aktualizujmy.
2. Stosujmy się do ustalonych przez bank zasad bezpieczeństwa zamieszczonych na stronie. Jeśli coś odbiega od normy, to przerwijmy transakcję i skontaktujmy się z bankiem. Kupujmy tylko w takich sklepach internetowych, gdzie jest szyfrowane połączenie – widzimy kłódkę i odpowiedni certyfikat, najlepiej znanych nam już wcześniej.

3. Dokonujmy płatności tylko z własnego komputera lub telefonu. Nie korzystajmy z publicznej sieci np. na lotnisku, w kawiarence internetowej. Nie wchodźmy na stronę banku z linku w wyszukiwarce, lecz wpisujmy adres ręcznie. Tak samo postępujmy z numerem konta odbiorcy naszego przelewu.
4. 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!
5. Nie oszczędzajmy, instalując na komputerze nielegalne oprogramowanie. Może ono zawierać przygotowane przez hakerów wirusy, które pomogą im w opanowaniu naszego komputera, wyłudzeniu danych, i w końcu pozwolą na okradzenie nas.
6. Nie otwierajmy wiadomości i dołączonych do nich załączników z nieznanych źródeł. W załącznikach może być ukryte złośliwe oprogramowanie.
7. Nie wchodźmy na podejrzane strony, np. strony z treścią pornograficzną. To także źródło wirusów.
8. Skanujmy od czasu do czasu nasz komputer, szczególnie przed zalogowaniem się na stronę banku.
9. Regularnie aktualizujmy oprogramowanie na komputerze, szczególnie oprogramowanie przeglądarek internetowych. Hakerzy szukają luk, a producenci cały czas „uszczelniają” wykryte luki w oprogramowaniu. Dzięki aktualizacjom mamy zawsze na komputerze najbardziej odporne na ataki hakerskie oprogramowanie.
10. Zmieniajmy regularnie hasła do swojego komputera, hasła dostępu do konta internetowego. Powinny to być hasła trudne i różne do każdej usługi internetowej.

Image not found or type unknown

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na **www.bde.wib.org.pl**

Jak tworzyć bezpieczne hasła?

Hasła, które tworzymy do naszych internetowych kont mają za zadanie chronić nasze dane i zapewnić nam bezpieczeństwo w sieci. Jednak według badań 50 proc. Polaków nie zmienia regularnie pin-u i hasła do bankowości internetowej. Tworzymy też hasła bardzo łatwe do złamania przez przestępców internetowych. A jak tworzyć bezpieczne

hasła?

Ustaw silne hasło

- Silne hasła to takie, które składają się z wielkich i małych liter, cyfr i znaków specjalnych.

- Trudne do wykrycia są hasła nie związane z charakterystycznymi danymi, które można przypisać do danej osoby, np. miejscem urodzenia, imieniem bliskiej osoby itd.

Jakie hasła nie są bezpieczne?

- Hasła poniżej 8 znaków

- Hasła będące imieniem lub nickiem

- Zbiór samych cyfr

- Hasło bez znaków specjalnych

- Hasło wykorzystane w wielu serwisach

Kiedy użytkownik proszony jest o wymyślenie hasła zawierającego DUŻĄ literę - w 90% przypadków będzie to pierwsza litera wyrażenia.

Jeśli poproszony jest o zastosowanie w swoim haśle cyfr:

- zazwyczaj użyje dwóch cyfr - pewnie będzie to rok urodzenia,
- kolejnym częstym wyborem jest zastosowanie na końcu wyrazu czterech cyfr – często jest to aktualny rok kalendarzowy,
- popularne zakończenie hasła to jedna cyfra – często 1, a następnie w kolejności są 3 cyfry.

Gdy potrzebujemy użyć znaku specjalnego – to chętnie wybieramy **!**

Takie przyzwyczajenia pozwalają przewidzieć hakerom jakiej struktury hasła używamy.

Jak stworzyć bezpieczne hasło?

- Powinno się ono składać z przynajmniej 8 znaków

- Powinno zawierać małe i wielkie litery (Aa, Bb, Cc...), cyfry (1234567890) oraz znaki specjalne (!@#$%^&*)

Niektóre znaki specjalne i cyfry są podobne do liter i można ten fakt wykorzystać przy tworzeniu silnego hasła, np.:

I = !

a = @

E = 3

S = $

O = 0

Do budowy hasła może posłużyć ulubione zdanie, np.:

ŻYRAFY WCHODZĄ DO SZAFY, PAWIANY WCHODZĄ NA ŚCIANY

Następnym krokiem jest wybranie pierwszych liter do stworzenia hasła:

ŻYRAFY **W**CHODZĄ **D**O **S**ZAFY, **P**AWIANY **W**CHODZĄ **N**A **Ś**CIANY

Na koniec zamieniamy litery na znaki specjalne, dodajemy cyfry oraz inne elementy bezpiecznego hasła:

ZWDSPWNS → 29ZwdPwn85

Dodane cyfry są zmodyfikowanym i rozdzielonym rokiem (1985), gdzie cyfra 1 została zastąpiona cyfrą 2.

Alternatywnym rozwiązaniem jest manager haseł, który jest programem komputerowym tworzącym i przechowującym mocne hasła (składające się z przypadkowych znaków).

Regularnie zmieniaj hasło

- Zrób z tego nawyk (zmieniaj je np. pierwszego dnia każdego miesiąca razem z opłacaniem rachunków)

- Jeśli masz problemy z zapamiętaniem hasła, nie musisz zmieniać całego hasła - wystarczy, że w jakiś sposób je zmodyfikujesz

Stosuj różne hasła do różnych serwisów

- Nie używaj tego samego hasła do wielu serwisów (np. do bankowości internetowej, poczty e-maila czy serwisów społecznościowych). Jeśli któreś z kont zostanie przejęte przez hackera, pozwoli to uchronić twoje pozostałe dane.

- Profiluj trudność hasła do tego, jak ważne dla Ciebie informacje ono chroni.

- Wyłącz automatyczne zapamiętywanie haseł w swojej przeglądarce internetowej.

- Nie zapisuj nigdzie swoich haseł i numerów

Dbajmy o swoje bezpieczeństwo w sieci!

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę www.bde.wib.org.pl

Jak bezpiecznie korzystać z kart płatniczych

Karta płatnicza staje się poza gotówką coraz częstszym „wyposażeniem” naszego portfela. W przypadku kradzieży karty złodziej, aby wypłacić pieniądze z bankomatu lub dokonać transakcji w sklepie musiałby znać nasz kod PIN.

Wyjątkiem od tej reguły są transakcje na kwoty poniżej 50 złotych metodą zbliżeniową (bez wprowadzania kodu PIN).

PIN to klucz do naszego skarbca

Aby kod PIN mógł być skuteczną obroną przed kradzieżą naszych pieniędzy musimy przestrzegać kilku zasad.

Kod PIN możemy znać tylko my. To oznacza, że nie powinniśmy nikomu dawać naszej karty po to, aby wypłacił dla nas pieniądze z bankomatu lub zrobił zakupy.

Kod musimy pamiętać. Nie powinniśmy go zapisywać, a jeśli musimy to w bezpiecznym miejscu, a cyfry kodu powinny być tak zapisane, aby nikt postronny nie mógł się domyślić, co one oznaczają. W żadnym wypadku nie przyklejajmy karteczek z kodem PIN do karty płatniczej, nie wkładajmy kodu zapisanego na karteczce do portfela, ani nie zapisujmy go w telefonie komórkowym, ponieważ w przypadku kradzieży wszystkie te przedmioty mogą znaleźć się w posiadaniu złodzieja.

Przestępca może również próbować odgadnąć nasz PIN, nie wybierajmy więc takich ciągów cyfr jak np. 1234 lub 1111, albo roku naszego urodzenia, który złodziej może znać, jeśli poza kartą ukradnie nam także dowód osobisty. Wtedy koniecznie pamiętajmy o zastrzeżeniu naszego dokumentu w swoim banku lub pod ogólnopolskim numerem (+48) 828 828 828, aby ustrzec się przed zaciągnięciem na nasze konto kredytu w banku!

Chrońmy swój kod PIN

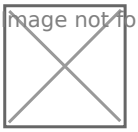
Nikt nie powinien widzieć jaki kod PIN wpisujemy na klawiaturze bankomatu, albo na terminalu w sklepie czy w restauracji. Czasami przestępcy umieszczają w bankomatach kamery. Dlatego na wszelki wypadek, kiedy wpisujemy PIN na klawiaturze, powinniśmy tę klawiaturę zasłaniać drugą ręką. Podobnie powinniśmy się zachowywać w sklepie.

Nie traćmy karty z oczu nawet na chwilę

W restauracji nie powinniśmy dawać karty kelnerowi, aby użył jej gdzieś na zapleczu. Obecnie w restauracjach są przenośne terminale POS i obsługa umożliwia nam płacenie przy stoliku. Jeśli w restauracji nie ma przenośnego terminala powinniśmy dokonać płatności przy kasie, cały czas obserwując osobę, która ma naszą kartę w swoich rękach. Nie możemy dopuścić do sytuacji, w której tracimy kartę z oczu nawet na chwilę, aby nie dopuścić do skopiowania danych z karty, za pomocą których przestępca mógłby dokonać płatności w Internecie.

Stracisz kartę – natychmiast ją zastrzeż

Posiadacz karty powinien ją natychmiast zastrzec w momencie kiedy zorientuje się, że ją zgubił lub mu ją ukradziono. Karty płatnicze można zastrzec w oddziale banku lub telefonując na infolinię banku, albo dzwoniąc pod ogólnopolski numer (+ 48) 828 828 828.



Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na **www.bde.wib.org.pl**

Jak bezpiecznie kupować w sieci

Ruch w sieci internetowej, tak jak ruch drogowy, wymaga od nas przestrzegania pewnych reguł bezpieczeństwa.

Nikt rozsądny nie przechodzi przez ulicę przy czerwonym świetle. Jeśli nie ma sygnalizacji świetlnej, to przed przejściem należy spojrzeć w lewo, potem w prawo,

jeszcze raz w lewo i po stwierdzeniu, że nie nadjeżdża żaden pojazd, może spokojnie przejść na drugą stronę ulicy. Tak samo nikt rozsądny nie daje nieznanej osobie swojego portfela z pieniędzmi. A właśnie tak często robimy w Internecie, kiedy nie przestrzegamy podstawowych zasad bezpieczeństwa i przelewamy swoje pieniądze na konta przestępców lub też dajemy im dostęp do naszych wrażliwych danych, i w ten sposób pozwalamy się okraść.

Bezpieczny komputer – to podstawa

Jeśli decydujemy się robić zakupy w sieci, to też musimy zadbać o swoje bezpieczeństwo. Przede wszystkim nasz komputer musi być bezpieczny. Na bezpieczeństwo naszego komputera składają się dwa elementy: nasze zachowanie w sieci i zainstalowane oprogramowanie.

Jeśli nie prowokujemy losu i nie wchodzimy na podejrzane strony, to jest wysoce prawdopodobne, że sami nie ściągniemy do swojego komputera złośliwego oprogramowania, które może ułatwić przestępcom okradzenie nas. Nie powinniśmy też sami instalować na komputerze oprogramowania z nieznanych źródeł czy nielegalnych kopii oprogramowania znanych firm.

Ważny program antywirusowy

Jeżeli ostrożnie zachowujemy się w sieci, mamy legalne oprogramowanie, to jeszcze potrzebny będzie nam strażnik naszego komputera, czyli program antywirusowy, który chroni nas także przed oprogramowaniem szpiegującym. Co ważne nasz program antywirusowy musi być na bieżąco aktualizowany przez dostawcę tego programu. Koszt takiego rozwiązania to kwota ponad stu złotych w skali roku. Istnieje także darmowe oprogramowanie antywirusowe, które można ściągnąć z internetu. Do nas należy decyzja, które oprogramowanie wybrać. Płatne czy bezpłatne. Najlepszym wyjściem jest skorzystanie z rady kogoś kto już od dawna korzysta z komputera. Niektóre banki proponują swoim klientom oprogramowanie antywirusowe. Często można z niego korzystać przez kilka miesięcy, a potem kupić je po promocyjnej cenie.

Tak „uzbrojeni” możemy przystąpić do zakupów w internecie. Zakupy w sieci oznaczają, że zaczynamy wchodzić na strony, których do tej pory nie odwiedzaliśmy i nie wiemy czy są bezpieczne.

Nie ufaj linkom, załącznikom i wyszukiwarkom

Ważne jest to jak dotrzemy na taką stronę. Należy unikać wchodzenia na daną witrynę z linków, które otrzymujemy w wysyłanych do nas wiadomościach elektronicznych, ani też nie powinniśmy wchodzić na stronę klikając w znaleziony w wyszukiwarce adres. Może się bowiem okazać, że ktoś chce nas zwabić na stronę o podobnej nazwie do tej, którą rzeczywiście jesteśmy zainteresowani. Dlatego za każdym razem powinniśmy

sami wpisywać w przeglądarkę adres sklepu czy serwisu, a nawet banku w którym mamy konto.

Kłódka i https

Przede wszystkim należy stwierdzić czy przy nazwie witryny, na której chcemy robić zakupy, widnieje napis https zamiast http. Powinniśmy także widzieć symbol kłódki, który oznacza bezpieczne połączenie internetowe. Były już jednak przypadki ataków na internautów przy użyciu autentycznych certyfikatów na fałszywych stronach. Aby wyeliminować to ryzyko należy kliknąć w symbol kłódki na witrynie i wyświetlić informacje na temat certyfikatu bezpieczeństwa danej witryny. Można także skorzystać z pomocy najpopularniejszej w Polsce wyszukiwarki internetowej Google. Wystarczy wkleić w wyszukiwarkę poniższy link i na końcu wpisać adres sprawdzanej strony.

http://www.google.com/safebrowsing/diagnostic?site=adres_strony

Sprawdzaj każdą nową witrynę

Jeśli zamierzamy po raz pierwszy kupić coś u danego sprzedawcy w internecie to warto sprawdzić jego dane kontaktowe i identyfikacyjne. Brak numeru telefonu, adresu e-mail lub adresu firmy powinien nas zaniepokoić. Warto też sprawdzić jakie metody płatności proponuje sprzedawca. Jeżeli jest to jedna metoda płatności i żąda się od nas zapłacenia z góry za dany towar to taka transakcja może być ryzykowna. Serwisy cieszące się uznaniem zwykle oferują możliwość zrealizowania zakupu na kilka sposobów np. z użyciem karty płatniczej, czy za pośrednictwem różnych banków jako szybkie i bezpośrednie płatności.

Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

Nie daj się wirusom i oszustom

W dobie epidemii koronawirusa ostrożność nie powinna się ograniczać jedynie do częstego mycia rąk czy unikania zgromadzeń. Poważnym zagrożeniem dla każdego z nas jest nie tylko groźna infekcja ale i przestępcy, którzy wykorzystują panikę towarzyszącą epidemii jako szansę dla oszukańczych działań.

Człowiek zatroskany o swoje życie, czy to doczesne, czy też wieczne, jest w stanie zrobić dosłownie wszystko, by zyskać choć trochę nadziei na ocalenie. Doskonale zdawał sobie z tego sprawę niejaki Sanderus, wędrowny szarlatan z sienkiewiczowskich „Krzyżaków", który za sowitą opłatą oferował… pióra z anielskich skrzydeł tudzież inne rzekome relikwie, mające według jego zapewnień chronić przed wiecznym potępieniem. Choć od czasów zwycięstwa pod Grunwaldem minęło przeszło sześć wieków, metody działania oszustów nie zmieniły się ani trochę. Złowrogie wiadomości o postępach koronawirusa i alarmistyczne doniesienia o kolejnych ofiarach powodują u nas wszystkich lęk i niepewność jutra. Bardzo pewnie czują się natomiast przestępcy, którzy już od pierwszych dni stanu zagrożenia epidemicznego prześcigają się w pomysłach, jak tu od naiwnych bądź przestraszonych ludzi wyłudzić jak najwięcej pieniędzy. Musimy o tym pamiętać, kiedy pewnego dnia do naszych drzwi zapuka obwoźny handlarz, oferujący „niezwykle skuteczne" środki medycyny ludowej, podejrzane mikstury czy wręcz amulety, ponoć odpędzające infekcje niczym siły nieczyste. Decydując się na zakup takich produktów, czy to od domokrążcy czy też w Internecie, ryzykujemy w najlepszym razie stratę pieniędzy, jako że substancje te są całkowicie nieskuteczne. W tym gorszym scenariuszu użycie rzekomych leków może dodatkowo spowodować poważne problemy zdrowotne, które bynajmniej nie będą efektem słynnego już koronawirusa. Pamiętajmy o jednym: dla przestępcy liczy się tylko i wyłącznie zysk. Cyniczny oszust nie będzie mieć żadnych skrupułów, by wprowadzić na rynek substancje niebezpieczne lub skażone, jeśli tylko skutecznie przekonać ludzi, że kupują życiodajne lekarstwo.

Najskuteczniejszym sposobem na pokonanie wirusa jest opracowanie dobrej szczepionki, nad czym pracują największe laboratoria medyczne świata. Firmy te dysponują wielomiliardowymi budżetami na badania, a postęp prac sponsorowany jest przez rządy wielu państw i najbogatszych ludzi świata. Tymczasem w Internecie nie brakuje zachęt, byśmy i my, zwykli zjadacze chleba, dołożyli swój grosz do walki ze złowieszczym mikrobem. Takie ogłoszenia w istocie mają tylko i wyłącznie jeden cel: wyłudzenie pieniędzy. Dokonując przelewu na wskazane konto możemy być pewni, że nie przyspieszamy prac nad nową szczepionką nawet o sekundę, pomagamy natomiast bezwzględnemu oszustowi pozyskać środki, które przeznaczy na zakup luksusowego auta czy inne kosztowne zachcianki. Co gorsza, utrata pieniędzy przesłanych na złodziejskie konto nie musi oznaczać końca naszych problemów. Większość podejrzanych stron, również tych z pseudozbiórkami pieniędzy na prace nad szczepionkami, zawiera złośliwe oprogramowanie, które aktywuje się po kliknięciu we wskazany link. Konsekwencje zainfekowania laptopa bądź telefonu takim wirusem mogą być poważne, jego celem jest bowiem albo uzyskanie kontroli nad naszym rachunkiem bankowym, albo też przechwycenie naszych danych osobowych. W pierwszym przypadku można się spodziewać nawet wyczyszczenia całego rachunku i utraty oszczędności życia, z kolei skradzione dane osobowe przestępcy chętnie

wykorzystają, by wyłudzić kredyt lub pożyczkę. A my będziemy przez długi czas udowadniać, że nie jesteśmy przysłowiowym wielbłądem. Podobnie fatalne konsekwencje może mieć niewinne z pozoru kliknięcie w SMS-a lub maila, informującego o zmianach zasad świadczenia usług bankowych czy telekomunikacyjnych w związku z epidemią. Przestępcy potrafią również „poinformować" nas o możliwości bezpłatnego zamówienia maseczki czy subskrypcji informacji na temat zagrożenia epidemiologicznego, regularnie przychodzących na nasz telefon. Wszystkie takie wiadomości należy niezwłocznie kasować! Chwila nieuwagi może sprawić, że do końca epidemii dotrwamy wprawdzie w dobrym zdrowiu, ale za to z pustym kontem lub co gorsza z długami, wygenerowanymi przez nieznanych sprawców. A przecież – jak to śpiewała kiedyś Halina Kunicka – „lepiej bogatym i zdrowym, niż biednym i chorym być…"

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**