POLICJA
Komenda Miejska
Policji w Katowicach

Bezpieczn@ Przystań

KOMISARIAT I POLICJI ul. Żwirki Wigury 28 tel. 032 200-35-00 Punkt przyjęć dzielnicowych Katowice ul. Graniczna 57 tel. 32 / 255 26 14 Kierownik Rewiru Dzielnicowych tel.:200-35-42, 600-208-482	KOMISARIAT II POLICJI ul. Iłłakowiczówny 2 tel. 32 200-36-50 Punkty przyjęć dzielnicowych: 1. Katowice, ul. Słowiańska 1 Kierownik Rewiru Zespołu Dzielnicowych: tel.:200-36-61, 600-208-479
KOMISARIAT III POLICJI ul. Książęca 20 tel. 32 200-38-00 Kierownik Rewiru Dzielnicowych: tel.: 200-38-35, 600-208-488	KOMISARIAT IV POLICJI ul. Policyjna 7 tel. 32 200 -37-51 Kierownik Rewiru Dzielnicowych tel.: 200-37-79, 300-208-485
KOMISARIAT V POLICJI ul. Lwowska 7 tel. 032 200-37-00 Punkty przyjęć dzielnicowych Katowice, ul. 1-go Maja 122 Kierownik Rewiru Dzielnicowych tel.: 200-37-30, 600-208-560	KOMISARIAT VI POLICJI ul. Stawowa 8 tel. 32 200-38-50 Zespół Dzielnicowych tel.: 200-38-82
KOMISARIAT VII POLICJI ul. Tysiąclecia 5 tel. 32 200-39-00 Punkty przyjęć dzielnicowych Katowice, ul. Witosa 17 (tel. 32 / 204 40 50) Kierownik Rewiru Dzielnicowych 200-39-31, 600-208-497	Komenda Miejska Policji w Katowicach ul. Lompy 19 **telefony alarmowe: 997, 112** **www.katowice.slaska.policja.gov.pl**

Bezpieczeństwo w domu

Najlepszą gwarancją bezpieczeństwa i zabezpieczenia Twojego mienia jest dobry sąsiad.

- Będąc w domu zawsze zamykaj drzwi wejściowe na zamek.
- Strzeż swojej prywatności, po zmroku zasłaniaj zasłony, żaluzje w oknach.
- Nie otwieraj drzwi bez sprawdzenia kto i po co przyszedł. Bez otwierania drzwi spójrz przez wizjer i zapytaj kim jest. Jeśli podaje się za przedstawiciela jakiejś instytucji np. administracji, elektrowni, gazowni, banku itp. Zażądaj okazania legitymacji zawodowej lub identyfikatora. Telefonicznie zweryfikuj jego tożsamość w danej instytucji.
- Przyjmowaną osobę cały czas obserwuj i nie zostawiaj samej w mieszkaniu.
- Najbezpieczniejszym miejscem przechowywania Twoich oszczędności jest bank. Przechowując w domu pieniądze schowaj je w miejscu trudno dostępnym dla innych, nie mów o tym nikomu. Dyskrecja to podstawowa zasada ochrony siebie i swojego mienia.
- Nie pozostawiaj w zasięgu wzroku cennych rzeczy oraz ważnych dokumentów (np. portfela, kluczyków do samochodu, kluczy do mieszkania, saszetki z dokumentami, itp.).
- Nie przekazuj pieniędzy akwizytorom czy inkasentom i nie podpisuj z nimi żadnych umów. Poproś o zostawienie dokumentacji i przeanalizuj ją dokładnie, wspólnie z kimś zaufanym.
- Nie podawaj przez telefon swoich danych personalnych, numerów dokumentów, kont bankowych i haseł do nich, numerów karty bankomatowej i jej PIN-u, nie rozmawiaj o planach życiowych swoich, członków rodziny i znajomych.
- Bądź ostrożny w kontakcie telefonicznym z osobami, które telefonicznie podają się za członków Twojej rodziny, prosząc o gotówkę próbują wyłudzić od Ciebie pieniądze. Natychmiast, powiadom o tym Policję.

- Oszuści często próbują wzbudzić litość osób starszych poprzez prośby o szklankę wody czy kromkę chleba. Nie wpuszczaj obcych osób do mieszkania. Jeżeli ktoś źle się czuje i potrzebuje pomocy udziel jej na korytarzu, wezwij karetką. Osoby żebrzące odsyłaj do instytucji pomocowych czy urzędu miasta.
- Bądź przygotowany na nieprzewidziane sytuacje, które mogą wydarzyć się w nocy - w pobliżu łóżka połóż niezbędne leki, latarkę i telefon.

Oszustwa metodą „Na wnuczka”

Dobre serce, łatwowierność, naiwność, a czasem także zwykłą bezmyślność starszych ludzi coraz częściej wykorzystują pozbawieni skrupułów oszuści.

Telefonujący oszust podaje się za wnuczka(ę), opowiada o:

- wypadkach drogowych, transakcjach finansowych, zakupie nieruchomości, konieczności zwrotu długu, porwaniu itp.
- przekazuje informację, że jedynym sposobem na "załatwienie" sprawy i uniknięcie odpowiedzialność jest przekazanie pieniędzy za pośrednictwem przysłanego przyjaciela lub podstawionego kuriera.

Pamiętaj!

- Oszust spróbuje zdobyć Twoje zaufanie i wpłynąć na emocje. Dla uwiarygodnienia wykorzystuje informacje pozyskane podczas tej lub wcześniejszych rozmów.

Oszuści działający metodą "na wnuczka" wprowadzają swoje ofiary w błąd, podając się za członka rodziny. Coraz częściej podszywają się także pod osoby zaufania publicznego - policjanta, prokuratora, czy księdza. Fałszywy mundurowy twierdzi, że oszust został namierzony i prosi o pomoc w jego zatrzymaniu. Nalega, aby senior wypłacił

pieniądze z banku i przekazał je wyznaczonej osobie lub przelał na wskazany numer konta. Przekonuje, że pomoże to w schwytaniu przestępców. Zdarza się również, że grozi odpowiedzialnością, w przypadku odmowy.

Pamiętajmy, w żadnym wypadku prawdziwi policjanci nie mogą żądać ani przyjmować pieniędzy za korzystne zakończenie sprawy. Stróże prawa również nigdy nie informują o prowadzonych przez siebie sprawach telefonicznie.

Jak się ustrzec przed oszustem?

Daj sobie czas do namysłu.
Rozmowę z osobą, która podaje się za Twojego wnuczka czy inną bliską osobę zakończ komunikatem typu:
"Nie mogę teraz podjąć decyzji. Muszę chwilę się zastanowić. Zadzwoń do mnie za pół godziny".

Skontaktuj się z bliskimi
Nie trzymaj informacji w tajemnicy - zweryfikuj jej prawdziwość. Upewnij się, czy rodzina rzeczywiście potrzebuje pomocy. Twoje bezpieczeństwo jest najważniejsze.

Powiadom Policję
Jeżeli masz wrażenie, że ktoś próbuje Cię oszukać, natychmiast powiadom o tym Policję.
Zadzwoń na bezpłatny numer alarmowy **112**.
Przekaż dyżurnemu informacje o swoich podejrzeniach.

Bezpieczeństwo na ulicy i w środkach komunikacji publicznej

- Uważaj na kieszonkowców! Nie trzymaj pieniędzy i dokumentów w jednym miejscu, porozkładaj je do różnych części ubrania. Noś przy sobie tylko niezbędną ilość gotówki.
- Torebkę noś na krótkim pasku, przewieszoną przez ramię i mocno przyciśniętą do ciała. Złodziejowi będzie ją trudniej wyrwać.
- Unikaj samotnego poruszania się po zmroku. Poproś znajomych, by odprowadzili Cię na przystanek lub rozważ możliwość skorzystania z taksówki. Poruszaj się po drogach ruchliwych i dobrze oświetlonych, omijając ciemne zaułki, przejścia podziemne. Powstrzymaj pokusę wracania na skróty, zwłaszcza przez ciemne skwery, bramy czy podwórza.
- Widząc zbliżającą się grupę ludzi, których zachowanie lub wygląd wzbudza Twój niepokój, przejdź na drugą stronę ulicy. Przybierz odpowiednia postawę - wyprostuj się, idź stanowczym krokiem i staraj się sprawiać wrażenie opanowanego i pewnego siebie. Unikaj kontaktu wzrokowego z nieznajomymi!
- Jeśli ktoś zaczepia Cię na ulicy, szczególnie w nocy, zachowaj bezpieczną odległość. Nie pozwól zbliżyć się nieznajomemu do siebie bliżej niż na wyciągnięcie ręki.
- Nie zawieraj przypadkowych znajomości. Nie korzystaj z ofert podwiezienia samochodem do domu przez osoby nieznajome, sam również nie zabieraj przypadkowych pasażerów.
- Nie korzystaj z poczęstunku oferowanego przez przygodnie poznane osoby - w ten sposób złodzieje często usypiają swoje ofiary.
- Podróżując środkami komunikacji publicznej zwracaj uwagę na posiadany bagaż, zachowaj szczególną czujność podczas wsiadania i wysiadania.
- Zajmuj miejsce w gronie pasażerów wzbudzających zaufanie (np. rodziny z dziećmi) lub blisko kierowcy, motorniczego czy drużyny konduktorskiej.

Bezpieczeństwo w sklepie, w banku, na poczcie, przy bankomacie

- Będąc w sklepie pamiętaj, aby robione zakupy nie odwróciły Twojej uwagi od rzeczy osobistych. Nie zostawiaj torebki, czy saszetki bez opieki w wózku sklepowym.
- Płacąc za zakupy unikaj okazywania zawartości portfela. Korzystaj z wcześniej odliczonej gotówki. Dyskretnie chowaj portfel czy kartę płatniczą.
- Podchodząc do bankomatu rozejrzyj się, czy ktoś cię nie obserwuje. Zwróć uwagę czy na klawiaturze i czytniku karty nie są zamontowane dodatkowe elementy, które skopiują dane z Twojej karty.
- Dyskretnie wprowadzaj kod PIN, aby inni nie mogli go zauważyć. Nie umieszczaj numeru PIN na karcie! Przechowywanie zapisanego PIN-u wraz z kartą grozi utratą pieniędzy.
- W przypadku konieczności wypłaty z konta większej kwoty pieniędzy - skorzystaj z eskorty rodziny lub kogoś zaufanego. Unikaj noszenia przy sobie dużej ilości gotówki. Duże transakcje realizuj za pośrednictwem banku.

„Umowy, pożyczki….
Sprawdź zanim podpiszesz”

Różne firmy kuszą wygodą: oferują szybki i łatwy dostęp do gotówki w formie pożyczki na dowód, przez Internet, na sms, bez zabezpieczeń, a nawet z dowozem do domu. Ale uwaga - za to wszystko trzeba zapłacić najwyższym na rynku oprocentowaniem i kosztami zaciągniętego zobowiązania!

- Zachowaj szczególną ostrożność podczas zawierania umów finansowych, w tym przede wszystkim zaciągania wysoko oprocentowanych, krótkoterminowych pożyczek tzw. „chwilówek" oraz korzystania z usług finansowych, które nie podlegają szczególnemu nadzorowi państwa.
- Pożyczki udzielane pod hasłem „bez BIK", „nawet z komornikiem", „dla osób ze złą zdolnością kredytową", skierowane do konsumentów, którzy mieli w przeszłości problemy z terminową spłatą swoich zobowiązań i osób którym banki odmawiają udzielenia kredytu są zwykle bardzo kosztowne.
- Konsument decydując się na zaciągnięcie kolejnej „szybkiej pożyczki" ryzykuje wejściem w tzw. spiralę zadłużenia. A wtedy zwykle nie da się już uniknąć egzekucji komorniczej.

Chcesz zaciągnąć bezpieczną pożyczkę? Zapamiętaj zasady:

Sprawdź wiarygodność firmy

Listę podmiotów objętych nadzorem finansowym można znaleźć na stronie: www.knf.gov.pl lub na stronie internetowej kampanii: www.zanim-podpiszesz.pl. Dodatkowo, informacji o podmiotach objętych nadzorem finansowym można uzyskać pod bezpłatnym numerem infolinii Komisji Nadzoru Finansowego (tel. 800 290 479)

Uważaj pod czym się podpisujesz. Policz całkowity koszt pożyczki

Koszt pożyczki może się okazać znacznie wyższy, niż oczekujesz. Sprawdź jaka jest całkowita kwota do zapłaty. Każdy podmiot udzielający pożyczki zobowiązany jest do poinformowania o wysokości rzeczywistej rocznej stopy oprocentowania pożyczki (RRSO) oraz o całkowitej kwocie do zapłaty.

Możesz także samodzielnie policzyć koszt pożyczki za pomocą kalkulatora dostępnego na stronie internetowej www.zanim-podpiszesz.pl.

Dokładnie przeczytaj umowę

Szczególnie zwróć uwagę na następujące elementy:

- czy oprocentowanie pożyczki nie jest znacznie wyższe niż inne oferty na rynku;
- czy firma wymaga wniesienia wysokiego zabezpieczenia pożyczki zanim pożyczka zostanie udzielona – brak terminowego spłacania pożyczki może się wiązać z utratą zabezpieczenia, którego wartość najczęściej znacznie przewyższa kwotę zadłużenia albo które może mieć dla nas wartość sentymentalną;
- czy zapisy umowy uprawniają firmę do wyznaczenia zabezpieczenia w przyszłości;
- czy pojawiają się dodatkowe opłaty zapisane w umowie, np. za rozpatrzenie wniosku, za wydanie decyzji, prowizje, opłaty za wizyty przedstawiciela pożyczkodawcy w domu, ubezpieczenia –suma tych opłat może znacznie podwyższać koszt pożyczki.

Pytaj o szczegóły

Jeżeli nie rozumiesz jakiegoś zapisu w umowie, poproś o wyjaśnienie. W wypadku wątpliwości poproś o wzorce dokumentów i skonsultuj je z prawnikiem lub inną zaufaną osobą.

Bezpieczne oszczędności.

Chcesz bezpiecznie ulokować pieniądze?Zapamiętaj cztery zasady:

Sprawdź, czy firma objęta jest nadzorem państwowym

Czy podmiot gromadzący pieniądze jest nadzorowany przez Komisję Nadzoru Finansowego?

Listę podmiotów objętych nadzorem finansowym można znaleźć na stronie: www.knf.gov.pl lub na stronie internetowej kampanii: www.zanim-podpiszesz.pl.

Pamiętaj, że wysoki zysk to zawsze duże ryzyko

Czy obiecany zysk znacznie przekracza inne oferty na rynku?

- inwestując swój kapitał ponosisz ryzyko nie tylko nieuzyskania oferowanego zysku, ale wręcz utraty części bądź całości wpłaconych pieniędzy.
- sytuacja taka jest tym bardziej prawdopodobna, im większy zysk jest obiecywany.

W praktyce najbezpieczniejsze inwestycje to lokaty w bankach lub obligacje emitowane przez Skarb Państwa.

Dokładnie przeczytaj umowę

Szczególnie zwróć uwagę na następujące elementy:

- czy firma wymienia okoliczności, w których nie wypłaci części bądź całości przyjętych pieniędzy,
- czy w umowie występuje obowiązek poniesienia opłaty za przechowanie pieniędzy.

Przy występowaniu wspomnianych klauzul w umowie należy rozważyć celowość korzystania z usług takiej firmy i powierzania jej

swoich pieniędzy. Warto pytać o szczegóły. W wypadku wątpliwości należy poprosić o wzorce dokumentów i skonsultować je z prawnikiem lub inną kompetentną osobą.

Nie podpisuj, jeśli nie rozumiesz

Nie należy korzystać z usług finansowych, których się nie rozumie. Jeśli oferujący usługi nie chce lub nie potrafi wyjaśnić ich zasad, lepiej zrezygnować z takiej propozycji.

Materiał dot. bezpiecznego korzystania z usług finansowych opracowano na podstawie informacji zawartych na stronie: www.zanim-podpiszesz.pl

Bezpieczne korzystanie z telefonu komórkowego

- Telefon noś zawsze przy sobie w miejscu trudno dostępnym dla kieszonkowców.
- Podczas pobytu na basenie, zajęć sportowych, zabiegów rehabilitacyjnych czy badań lekarskich oddaj telefon do bezpiecznego depozytu.
- Unikaj pokazywania telefonu innym. Staraj się ograniczyć rozmowy przez telefon w miejscach publicznych. W ten sposób demonstrujesz posiadany sprzęt i wskazujesz złodziejowi miejsce jego przechowywania.
- Zapisz numer identyfikacyjny twojego telefonu tzw. IMEI (aby go sprawdzić wpisz na klawiaturze telefonu kod: *#06#), w razie utraty sprzętu będzie on potrzebny do jego odzyskania.
- Po stwierdzeniu kradzieży telefonu, natychmiast poinformuj o tym Policję i operatora- zablokuje on konto.
- Kupując telefon komórkowy sprawdź jego legalność – zażądaj od sprzedawcy oryginalnego pudełka, akcesoriów oraz dokumentów i dowodu zakupu.
- Ostrożnie korzystaj z wszelkich ofert konkursowych polegających na wysłaniu sms-a zwrotnego czy oddzwonieniu.

Najpierw sprawdź cennik. Opłata za skorzystanie z takiej oferty może być bardzo wysoka.

BEZPIECZENSTWO SENIORA W SIECI

Z roku na rok coraz więcej osób w wieku 65+ korzysta z Internetu. Pamiętaj! Sieć to przyjemność odkrywania nowych witryn, ale niekiedy także zagrożenie. Jak bezpiecznie poruszać się w Internecie? Jak ochronić się przed działaniami cyberprzestępców?

Zacznijmy od kilku prostych, ale bardzo ważnych zasad:

- **pomyśl, zanim klikniesz** – nie klikaj wszystkich łączy w portalach społecznościowych i unikaj klikania w nagłówki z sensacyjnymi, przykuwającymi uwagę tytułami.
- **stosuj oprogramowanie zabezpieczające** – upewnij się, że zainstalowałeś oprogramowanie zabezpieczające we wszystkich komputerach i urządzeniach mobilnych, również w smartfonach i tabletach.
- **nie dodawaj nieznajomych** – jeśli w portalu społecznościowym ktoś, kogo nie znasz, chce dołączyć do Twoich znajomych, nie akceptuj zaproszenia – najpierw sprawdź skąd się znacie i dlaczego szuka kontaktu. Tak samo jak nie wpuściłbyś do domu obcej osoby.
- **zwolnij i zastanów się** – zanim klikniesz na link, otworzysz załącznik, udostępnisz informacje osobiste lub dane bankowe, zastanów się dwa razy. Jeśli coś nie wydaje Ci się stuprocentowo wiarygodne, wycofaj się i anuluj zadanie.

Podstawowe zasady bezpieczeństwa online

- **Chroń swoje dane osobowe.** Są one niezwykle cenne. Aby zminimalizować ryzyko kradzieży tożsamości, nie udzielaj nikomu swoich danych osobowych, jeżeli nie masz pewności jak będą wykorzystane i chronione. Nie odpowiadaj ani nie klikaj na odsyłacze w emailach z pytaniami o twoje dane osobowe.
- **Wiedz, z kim masz do czynienia.** Robiąc zakupy online, poszukaj fizycznego adresu i numeru telefonu sprzedawcy. Zadzwoń żeby sprawdzić, czy ten numer działa. Zanim pobierzesz bezpłatne oprogramowanie, przeczytaj drobny druk – niektóre programy zawierają w sobie szkodliwe oprogramowanie.
- **Korzystaj z oprogramowania antywirusowego i antyszpiegowskiego, jak również** z firewall, aktualizuj je regularnie. Szukaj programów antywirusowych, które usuwają wirusy lub poddają je kwarantannie oraz programów antyszpiegowskich, które mogą zlikwidować szkody wyrządzone przez spyware. Upewnij się, że firewall jest włączony i należycie skonfigurowany. Jeżeli firewall został dostarczony jako wyłączony, włącz go.
- **Skonfiguruj należycie swój system operacyjny i przeglądarkę internetową.** Wybierz dostatecznie mocne ustawienia bezpieczeństwa, aby zmniejszyć zagrożenie ze strony hakerów. Koniecznie regularnie aktualizuj system.
- **Chroń swoje hasła.** Przechowuj hasła w bezpiecznym miejscu i nie podawaj ich nikomu w internecie, emailem ani telefonicznie.
- **Sporządzaj kopie zapasowe ważnych plików.** Jeżeli przechowujesz w komputerze ważne pliki, skopiuj je na dysk ruchomy i przechowuj w bezpiecznym miejscu.

Jak zabezpieczać swój email

- **Przezornie korzystaj z emailu.** Email jest doskonałym sposobem utrzymywania kontaktu ze znajomymi i rodziną oraz jako narzędzie pracy zawodowej. Nawet jeżeli masz dobre oprogramowanie zabezpieczające na komputerze, twoi znajomi i rodzina mogą nie być tak samo chronieni. Uważaj, jakie informacje przekazujesz emailem. Nigdy nie wysyłaj informacji o karcie kredytowej, numeru ubezpieczenia społecznego ani innych danych osobowych emailem.
- **Nie odpowiadaj na spam.** Jeżeli nie rozpoznajesz nadawcy komunikatu email, nie odpowiadaj. Odpowiadając na spam po to żeby się wypisać, możesz się narazić na jeszcze więcej spamu.
- **Twórz skomplikowane adresy email.** Skomplikowany adres email utrudnia hakerom automatyczne wytworzenie twojego adresu, wysłanie spamu lub skierowanie innego rodzaju ataków na twój email. Tworząc swój adres email zadbaj, aby był łatwy do zapamiętania. Spróbuj używać liter, cyfr i innych znaków w niepowtarzalnej kombinacji. W miarę możliwości zastępuj litery cyframi. Przykład skomplikowanego adresu:

  Tomasz1Kowalski3!2@op.pl
- **Twórz inteligentne i mocne hasła.** Utrudnij hakerom złamanie twojego hasła. Możesz stworzyć inteligentne hasło umieszczając w nim wielkie i małe litery, cyfry, znaki specjalne i używając więcej niż 6 znaków. Przykład silnego hasła: Go1dM!n3
- **Obserwuj aktywność online swojej rodziny i znajomych.** Osobisty adres email powinni posiadać tylko twoi członkowie rodziny, znajomi i zaufani współpracownicy. Nie ogłaszaj swojego adresu email na stronach internetowych, forach dyskusyjnych czy w pokojach czatów. Ogłoszenie adresu email naraża na spam lub na przekazywanie twojego adresu emailowego innym osobom. Jeżeli chcesz zaabonować biuletyn lub zapisać się na stronie internetowej i otrzymywać

potwierdzenie emailem za transakcje online, najlepiej podawaj adres email, który nie jest powiązany z żadnymi danymi osobowymi.

- **Zachowaj ostrożność otwierając załączniki i pobierając pliki od przyjaciół i znajomych lub akceptując emaile spod nieznanych adresów.** Otwierając email i załączniki oraz przyjmując pliki od przyjaciół, znajomych i innych narażasz się na wirusy, robaki i trojany. Jeżeli zdecydujesz się pobrać pliki, upewnij się, że oprogramowanie zabezpieczające jest włączone i obserwuj uważnie wszelkie ostrzeżenia.
- **Zachowaj ostrożność korzystając z programów IM (komunikatorów).** Jeżeli używasz programu IM do łączności ze znajomymi i rodziną, uważaj wysyłając jakiekolwiek dane osobowe. Chroń się używając pseudonimu jako ekranowej nazwy użytkownika IM. Nigdy nie przyjmuj obcych do swoich grup IM.
- **Uważaj na oszustwa z użyciem phishingu.** Phishing polega na używaniu oszukańczych emaili i fałszywych stron internetowych, które udają prawdziwe firmy, aby zwabić niepodejrzewających niczego użytkowników i nakłonić ich do ujawnienia danych dotyczących prywatnego konta lub nazwy użytkownika i hasła. Dla własnego bezpieczeństwa, jeżeli otrzymasz email od firmy, w którym znajduje się odsyłacz do strony internetowej, upewnij się, że strona, którą zamierzasz odwiedzić jest autentyczna. Zamiast kliknąć prosto do sieci z treści emailu, otwórz oddzielną stronę w przeglądarce i odwiedź stronę tej firmy bezpośrednio, aby wykonać konieczne czynności. Możesz także sprawdzić, czy email rzeczywiście pochodzi od autentycznej firmy telefonując do niej bezpośrednio.
- **Nigdy nie wpisuj swoich danych osobowych na ekran wyskakujący.** Czasami phisher skieruje cię na stronę prawdziwej organizacji, ale następnie pojawi się nieuprawniony ekran wyskakujący stworzony przez oszusta z formularzem do umieszczenia danych osobowych. Jeżeli go wypełnisz, twoje dane osobowe znajdą się w rękach phishera. Zainstaluj

oprogramowanie przeciwdziałające wyskakiwaniu okien, aby zapobiec tego rodzaju atakom.

Bezpieczne zakupy w sieci

- **Wiedz, z kim masz do czynienia.** Zanim coś kupisz, sprawdź fizyczny adres i numer telefonu sprzedawcy. Przyda się na wypadek wątpliwości lub problemów.
- **Wiedz co kupujesz.** Przeczytaj opis produktu podany przez sprzedawcę oraz, chociaż to przykre, drobny druk. Sprawdź warunki ogólne. Czy możesz zwrócić zakup i dostać zwrot pieniędzy, jeżeli nie będziesz zadowolony? Kto zapłaci koszty przesyłki? Czy jest opłata za zwrócenie towaru (restocking fee)? Wydrukuj i przechowaj zapisy swoich transakcji online, w tym emaile wymieniane ze sprzedawcą. Kupuj kupony na prezenty ze źródeł, które znasz i którym ufasz. Unikaj kupowania kart z witryn aukcyjnych, ponieważ mogą być fałszywe.
- **Oszczędnie udzielaj swoich danych osobowych.** Nie podawaj numeru karty kredytowej ani innych informacji finansowych w zamian za ofertę najnowszej technicznej zabawki, darmowego kuponu, sezonowej pracy czy wynajęcia lokalu na wakacje. Nie wysyłaj swoich informacji finansowych emailem. Email nie jest bezpiecznym sposobem przesyłania numerów – karty kredytowej, rachunku czekowego czy ubezpieczenia społecznego. Nie klikaj na odsyłacze w treści komunikatów email. Prawowite firmy nie pytają o dane finansowe za pomocą emailu ani komunikatów wyskakujących.
- **Sprawdzaj wytyczne dotyczące prywatności.** Koniecznie. Mogą być długie, lecz zawierają ważne informacje: np. jakie dane osobowe strona internetowa gromadzi, dlaczego i w jaki sposób będą one wykorzystane. Jeżeli nie możesz znaleźć wytycznych dotyczących prywatności lub zrozumieć ich – złóż zamówienie u kogoś innego i daj znać takiej witrynie, co o tym myślisz.

- **Porównuj ceny.** Jeżeli znasz producenta i numer modelu towaru, możesz porównywać „jabłka z jabłkami” u różnych sprzedawców. Niektórzy detaliści gotowi są obniżyć cenę do poziomu a nawet poniżej poziomu konkurentów. Wielu kupców oferuje w tym roku bezpłatną wysyłkę, lecz nie wszyscy – uwzględnij więc koszt przesyłki jako składnik ceny. Jeżeli zamawiasz online i odbierasz towar w sklepie, weź pod uwagę koszty parkowania lub komunikacji publicznej.
- **Czy powinieneś kupować, gdy masz połączenie za pomocą publicznego WiFi?** Nie wierz w to, że publiczne hot spoty są bezpieczne. Jeżeli nie możesz sprawdzić, czy dany hot spot skutecznie zabezpieczony, lepiej nie wysyłać przez taką sieć wrażliwych informacji takich jak numer karty kredytowej.
- **Płać kartą kredytową.** Oferują one najlepszą ochronę konsumentów. Na mocy przepisów federalnych masz prawo w niektórych okolicznościach zakwestionować opłaty i chwilowo zatrzymać zapłatę, gdy wierzyciel bada sprawę. Jeżeli twoja karta została użyta bez upoważnienia właściciela, jego odpowiedzialność cywilna jest zwykle ograniczona do pierwszych $50. Elektroniczne przekazywanie pieniędzy może być ryzykowne. Jest to tak jakbyś wysyłał gotówkę – nie sposób jej odzyskać. Kupowanie online za pomocą równoważników gotówki – karty debetowej, czeku osobistego, czeku kasjerskiego lub przekazu pieniężnego - może być ryzykowne. Używaj ich tylko, jeżeli wiesz z kim masz do czynienia.
- **To co darmowe może drogo kosztować**. Darmowe oszczędzacze ekranu, e-karty czy sezonowe okazje mogą ukrywać niebezpieczne wirusy. Dbaj, aby twoje oprogramowanie antywirusowe i przeciwko spyware, a także firewall były zawsze aktualne.
- **Obserwuj swoje konta finansowe.** Regularnie czytaj wyciągi bankowe, sprawdzaj czy odzwierciedlają opłaty, na które dałeś upoważnienie.

8 zasad bezpiecznego e-bankingu

1. Uważaj na fałszywe wiadomości e-mail.

Banki nigdy nie wysyłają do swoich klientów e-maili z prośbami o podanie poufnych informacji (uzupełnienie formularzy). Nie należy zatem odpowiadać na takie listy i nie uruchamiać zawartych w nich linków. Złodzieje często podszywają się pod bankowców i preparują korespondencję, a nawet witryny internetowe, które do złudzenia przypominają oryginały z banku. E-maile wysyłają do tysięcy osób w nadziei na złapanie naiwnego klienta, który dobrowolnie poda wrażliwe dane. W „imieniu banku" proszą o pilne zaktualizowanie informacji lub podanie kilku kodów jednorazowych z karty zdrapki w celu odblokowania rzekomo zablokowanego rachunku. Działania takie określa się terminem „phishing", który podchodzi od słowa „fishing" – łowienie. Dlatego każdą tego typu informację należy bezwzględnie zignorować i pod żadnym pozorem nie korzystać z linków przesłanych w e-mailu.

2. Sprawdź adres strony logowania.

Do logowania do systemu należy używać wyłącznie adresu podanego przez bank. Jeśli go zapomnimy, możemy sprawdzić w umowie z banku lub dostać się do systemu logowania bezpośrednio ze strony naszego banku. Nie powinno się używać w tym celu wyszukiwarki internetowej. Specjaliści odradzają także trzymanie strony logowania wśród „ulubionych" stron przeglądarki internetowej. Przestępcy tworzą bowiem oprogramowanie, które jest w stanie wykorzystać luki w systemie i podmienić stronę na fałszywą. O tym, że znajdujemy się na właściwej stronie internetowej, informuje nas pasek adresu. Adres

musi zaczynać się od https:// a przeglądarka powinna zweryfikować połączenie wyświetlając symbol zamkniętej kłódki.

3. Stosuj się do procedur własnego banku.

Logując się na stronę banku należy stosować się do procedur obowiązujących w danym banku. Na witrynie każdej instytucji znajduje się dokładna instrukcja, jak bezpiecznie przejść przez cały proces. Jeśli w trakcie logowania pojawią się komunikaty niezgodne z instrukcją, lub prośby o podanie kodów jednorazowych służących do zlecania przelewów, nie należy kontynuować procesu logowania. Powinno się natomiast niezwłocznie poinformować bank o zaistniałej sytuacji.

4. Aktualizuj system i przeglądarkę internetową.

Przeglądarka internetowa to program, który służy do otwierania stron internetowych, także tych do logowania do systemu bankowości internetowej. Należy zatem zadbać o to, by na naszym komputerze była zawsze najnowsza wersja tej aplikacji. Hakerzy wyszukują luk w programach, za pomocą których mogą wykraść niezbędne informacje. To samo dotyczy systemu operacyjnego, który powinien być na bieżąco aktualizowany. Dostawcy oprogramowania na bieżąco monitorują poziom bezpieczeństwa i publikują łatki uzupełniające luki w oprogramowaniu. Nowoczesna przeglądarka internetowa jest niezbędnym elementem zapewniającym bezpieczne korzystanie z systemu bankowości internetowej. Dobra przeglądarka powinna także ostrzec przed podejrzanymi witrynami:

5. Korzystaj z oprogramowania antywirusowego.

Równie niezbędne jak bezpieczna przeglądarka internetowa jest zainstalowanie programu antywirusowego. Tego typu aplikacja

powinna zapobiec instalacji wirusów i innego szkodliwego oprogramowania. Warto przy tym korzystać z programów polecanych przez ekspertów, ponieważ nie wszystkie aplikacje dostępne w sieci spełniają niezbędne standardy. Należy pamiętać, że instalowanie aplikacji pobranych z niesprawdzonych stron internetowych bardzo często kończy się zainfekowaniem komputera przez oprogramowanie szpiegujące. Warto także raz na kilka dni skanować antywirusem komputer i dbać o aktualne bazy wirusów.

6. Loguj się na własnym komputerze.

Zaletą bankowości internetowej jest to, że dostęp do własnego konta możemy mieć z dowolnego komputera podpiętego do sieci. Tu jednak zaleca się duża ostrożność – powinniśmy korzystać przede wszystkim z naszej własnej maszyny w domu. Nie powinniśmy logować się na ogólnie dostępnych komputerach, np. w kafejkach internetowych. Nie mamy bowiem gwarancji, że komputery te są „czyste". Mogą tam być zainstalowane programy szpiegujące, które potrafią przechwycić dane do logowania czy numery kart. Jeśli już jednak musimy skorzystać z obcego komputera należy pamiętać, by zawsze wylogować się z serwisu transakcyjnego.

7. Zapamiętaj dane i zmieniaj hasła.

Nie zapisuj danych do logowania w miejscach dostępnych osobom postronnym, a także bezpośrednio w przeglądarce internetowej. Staraj się także – jeśli to możliwe – okresowo zmieniać hasło dostępu do konta. Hasła jednorazowe do zatwierdzania transakcji internetowych trzymaj w bezpiecznym miejscu – nie zostawiaj ich na przykład w biurku w pracy. Pamiętaj, że są to dane, które mogą posłużyć do zlecenia przelewu z twojego konta. Sprawdzaj także daty i godziny ostatniego logowania na rachunek.

8. Pilnuj danych swojej karty.

Transakcje w sieci można dokonywać także za pomocą kart płatniczych. Podobnie jak w przypadku bankowości internetowej należy ignorować wszelkie e-maile z prośbą o podanie numerów kart. Nie należy korzystać z mało znanych sklepów internetowych, oraz ze sklepów, gdzie musimy podać dane na zwykłej, nie szyfrowanej stronie (brak https:// w adresie). W przypadku kart płatniczych newralgiczne dane to oprócz numeru kody CVV i CVV2 i PIN. Warto wiedzieć, że w bankach dostępne są specjalne karty przedpłacone do transakcji internetowych. Techniczny rachunek takiej karty można zasilić odpowiednią kwotą tuż przed dokonaniem transakcji. Karta nie jest powiązana z kontem bankowym, czy limitem kredytowym, nie istnieją zatem obawy, że jeśli dane wpadną w ręce niepowołanych osób, stracimy więcej pieniędzy.

Przy opracowaniu broszury wykorzystano informacje podane m.in. na stronach internetowych:
"Seniorzy na czasie"
Bankier.pl i inne.

Ważne telefony:

Pogotowie Ratunkowe	999, 112
Komenda Miejska Państwowej Straży Pożarnej, ul. Wojewódzka 11, 40-026 Katowice	998, 112
Pogotowie Energetyczne	991, 112
Pogotowie Gazowe	992, 112
Pogotowie Wodne	994, 112
Straż Miejska, 40-851 Katowice, ul. Żelazna 18	986
Miejski Rzecznik Konsumentów ul. Rynek 1,	(32) 20-68-010, (32) 2593-846
Pełnomocnik Prezydenta Miasta Katowice ds. Osób Niepełnosprawnych, ul. Rynek 1 , piętro VIII, pokój 805 A	(32) 25-93-212
Telefon Zaufania MOPS	32 256 92 78