Ministerstwo Rodziny
i Polityki Społecznej

AKTYWNI+

e-SENIOR

BEZPIECZEŃSTWO FINANSÓW W INTERNECIE


200
DWIEŚCIE ZŁOTYCH
NARODO
BANK
POLSKI
WARSZAWA
30 MARCA 2015 r.
PREZES
GŁÓWNY
SKARBNIK
BA9448987
WŁADYSŁAW II JAGIEŁŁO

Witam Państwa serdecznie,

Broszura, którą trzymają Państwo w rękach, została przygotowana przez Fundację „Idea dla Ciebie” jako część projektu „e-SENIOR” współfinansowanego przez Ministerstwo Rodziny i Polityki Społecznej w ramach programu „Aktywni+”. Projekt ten dedykowany jest zarówno dla osób, które nie miały do tej pory do czynienia z urządzeniami takimi jak komputer, tablet czy telefon typu smartfon, jak również dla tych, które są na początku tej drogi.

Zapraszam Państwa do zapoznania się z niniejszą publikacją w której w prosty i przystępny sposób przedstawione zostaną podstawowe informacje związane z tym, jak zadbać o bezpieczeństwo Państwa finansów w internecie.

Z wyrazami szacunku,

Agnieszka Janczura

Prezes Fundacji "Idea dla Ciebie"

Zapraszam na kanał YouTube „Idea dla Ciebie”, na którym znajdą Państwo filmy przygotowane z myślą o Seniorach pod następującymi tytułami:

1. Informatyka dla każdego - podstawy informatyki przedstawione w prosty i przystępny sposób.
2. Podstawy obsługi komputera.
3. Podstawy obsługi telefonu typu smartfon.
4. Komunikatory – nauka samodzielnego korzystania z komunikatorów do prowadzenia wideo rozmów, wysyłania i odbierania zdjęć i wiadomości tekstowych.
5. Jak korzystać z ciekawych aplikacji takich jak: YouTube, Facebook, Google Maps oraz Google Earth.
6. Jak założyć i korzystać z poczty e-mail?
7. Bezpieczeństwo finansów w internecie.
8. Zakupy przez internet - od zamówienia po odbiór w paczkomacie.

www.e-SENIOR.org.pl

W ramach projektu e-SENIOR powstała także strona internetowa, na której znajdą Państwo powyższe filmy, ale także niniejszy skrypt do samodzielnego pobrania i wydrukowania.

OSZUSTWA PRZEZ INTERNET

Generalnie ataki na użytkowników Internetu (poza szpiegostwem przemysłowym lub politycznym) mają na celu dwie rzeczy: kradzież pieniędzy lub kradzież danych (przy czym często kradzież danych z czasem również prowadzi do utraty pieniędzy).

Jest wiele sposobów, których mogą użyć oszuści do wyłudzenia od nas pieniędzy. Jednak większość z tych sposobów będzie wymagała podjęcia przez nas jakiegoś działania, dlatego też znając kilka podstawowych zasad dotyczących bezpieczeństwa w sieci mamy dużą szansę uchronienia się przed atakami hakerów.

Jak działają oszuści i jak się przed nimi uchronić?

Oszuści bardzo często w różny sposób wysyłają nam tak zwane linki i przekonują nas abyśmy w nie kliknęli. Linki są to przeważnie podkreślone niebieskie napisy. Kliknięcie w taki link przekierowuje (czyli prowadzi) nas na stronę, którą haker specjalnie przygotował, aby wyłudzić od nas np. nasze dane logowania do banku, poczty e-mail itd.

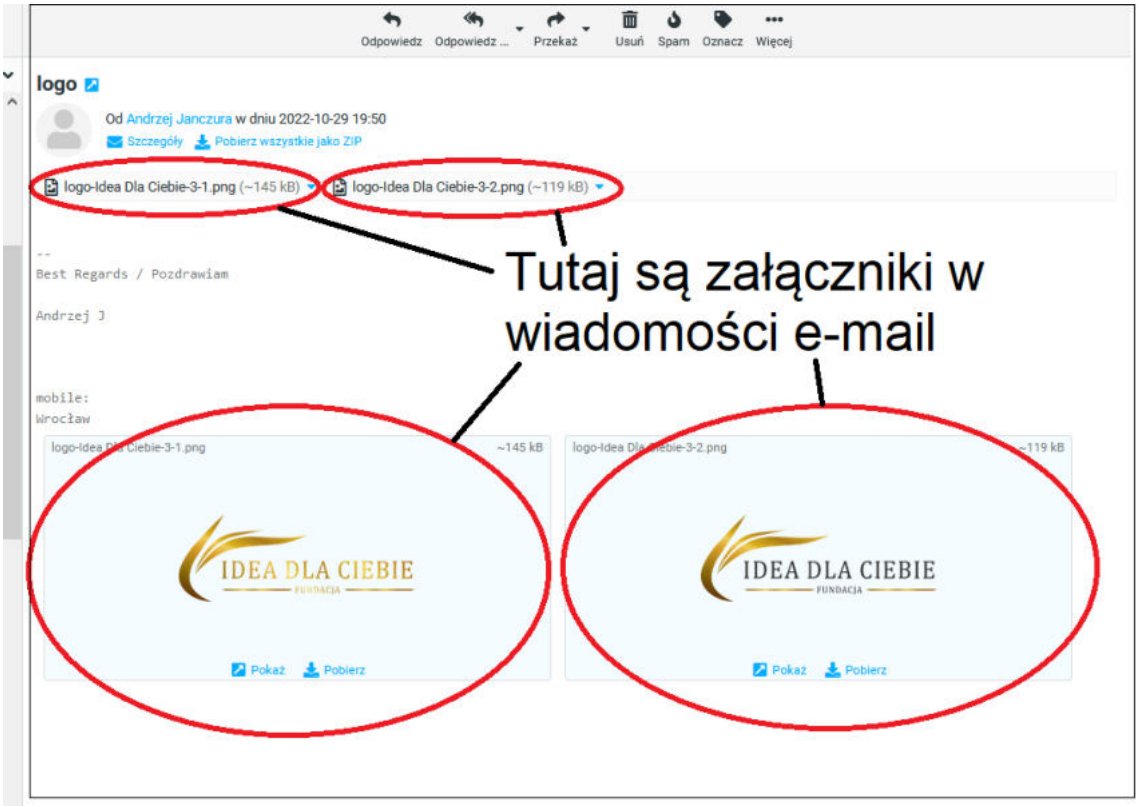
NIE KLIKAJ W LINKI!

Najprostszą więc rzeczą, która może nas uchronić przed oszustwem jest najzwyczajniej w świecie nieklikanie w te linki (czyli teksty, słowa napisane kolorem niebieskim i podkreślone) i to niezależnie od tego, czy dana wiadomość została wysłana do nas mailem czy sms-em.

Załączniki

Drugą złotą zasadą jest nieklikanie w załączniki. W filmie dostępnym na YouTube o tym, jak założyć pocztę e-mail ("Jak założyć i korzystać z poczty e-mail (G-mail)? #6") pokazane jest jak wysłać lub odebrać maila z załącznikiem. Załącznikiem tym może być zdjęcie, dokument czy dowolny plik. Jeżeli mail pochodzi od hakera to kliknięcie w nawet niewinnie wyglądające zdjęcie może uruchomić wirusa na naszym komputerze lub w naszym telefonie.

NIE KLIKAJ W ZAŁĄCZNIKI!



Fałszywe wiadomości

Niestety fałszywe załączniki możemy też dostać ze skrzynki pocztowej naszego znajomego. Jest to możliwe dlatego, że haker w bardzo prosty sposób może podszyć się pod dowolny adres mailowy. Czyli my będziemy widzieli w naszej poczcie, że mail przyszedł z autentycznego adresu osoby, którą znamy, jednak wiadomość ta będzie pochodziła od oszusta. Jeżeli nie czekamy na wiadomość od kogoś bliskiego, która powinna zawierać jakieś linki lub załączniki, a taką wiadomość dostaniemy, to bardzo dobrą praktyką przed kliknięciem w cokolwiek będzie po prostu zadzwonienie do tego znajomego i upewnienie się, że to naprawdę on wysłał tego maila czy tę konkretną wiadomość na nasz telefon.

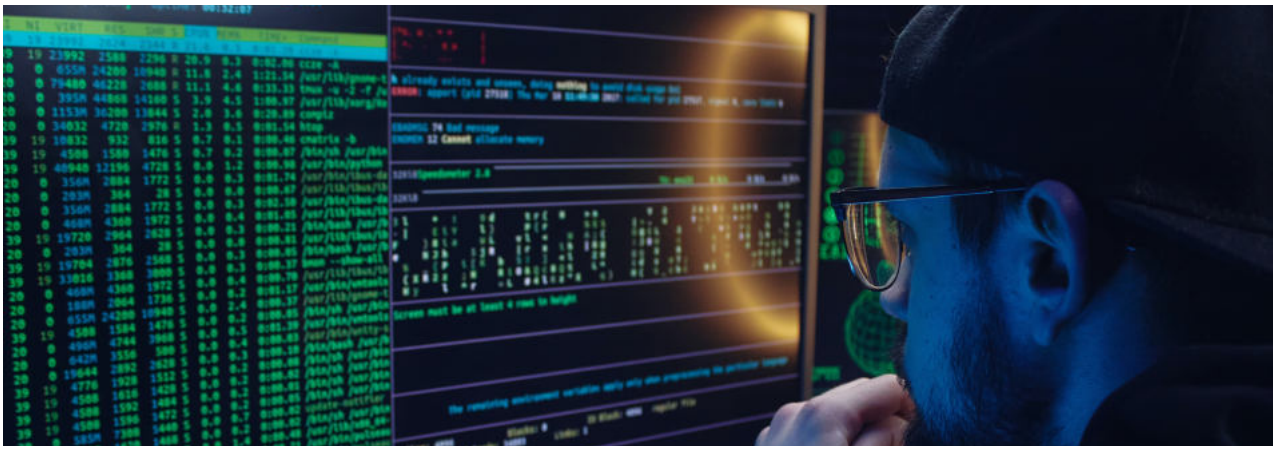
Hakerzy potrafią również podszywać się pod różne instytucje. Możemy dostać maila lub sms-a, który będzie wyglądał tak, jakby przyszedł z naszego banku, z Poczty Polskiej czy innego urzędu. Tutaj również zalecana jest daleko posuniętą ostrożność. Zanim klikniemy w jakikolwiek link najlepiej jeżeli skontaktujemy się z daną instytucją i potwierdzimy, że naprawdę wysłano z niej do nas jakąś wiadomość. Bardzo ważne przy tym będzie, aby nie dzwonić pod numer podany w tej wiadomości. Jeżeli jest to wiadomość od oszusta, to najprawdopodobniej wpisał on tam również inny, fałszywy numer telefonu.

źródło: bnpparibas.pl

Jeżeli chcemy potwierdzić czy wiadomość naprawdę została wysłana od danej instytucji sami znajdźmy numer do danego banku czy urzędu i zadzwońmy pod znaleziony przez nas numer.

Co to jest PHISHING?

Phishing to oszustwo polegające na tym, że haker tworzy fałszywe strony udające strony prawdziwych firm czy instytucji, służące do wykradania naszych loginów, haseł i innych ważnych danych.



Często można spotkać się z opinią, iż tym co gwarantuje nam, że strona jest bezpieczna jest zamknięta kłódka obok adresu strony internetowej oraz adres strony zaczynający się od "https" (ważny tutaj jest fakt, iż ten ciąg znaków zakończony jest literką "s"). Niestety obecność kłódki czy literki "s" na końcu http nie gwarantuje nam, że strona jest bezpieczna. Te dwa elementy gwarantują nam bezpieczne połączenie, to znaczy że „tunel" który w tym momencie łączy nasz komputer z daną stroną internetową jest bezpieczny i nikt z boku nie może zajrzeć do tego „tunelu", i odczytać tego co właśnie wpisujemy, ale bezpieczny tunel jak najbardziej może prowadzić do niebezpiecznej strony hakera. Czyli połączyliśmy się bezpiecznie z niebezpieczną, czy fałszywą stroną, która chce wykraść nasze dane.

Jakie wybrać dobre HASŁO?

Mówiąc o bezpieczeństwie warto wspomnieć o jeszcze jednej bardzo ważnej rzeczy. Pomimo, iż jest to trudne, to miejmy różne hasła do różnych kont. Do każdego banku powinno być inne hasło. Do każdego maila inne hasło itd. Pomóc nam może w tym manager haseł, jest to darmowa aplikacja. Dlaczego jest to tak ważne? Ponieważ z bardzo wielu instytucji czy firm wyciekły dane użytkowników. Z kilku banków, z sieci komórkowych itd. Jeżeli więc mieliśmy takie same hasło do poczty e-mail i takie samo do banku, to jeżeli dany operator maila został zhakowany, wówczas taki haker może używając naszego hasła do maila spróbować zalogować się do banku, innej skrzynki pocztowej czy na nasz profil na YouTube i prawdopodobieństwo, że mu się to uda jest bardzo duże. A jeżeli będziemy mieli róże hasła i to hasła bardziej skomplikowane, czyli zawierające duże i małe litery, cyfry czy znaki specjalne to znacząco utrudnimy hakerom życie.

Co to jest KLUCZ U2F?

Jest jeden sposób, który będzie w stanie zabezpieczyć nas przed phishingiem. Jest to tak zwany fizyczny klucz U2F. Wygląda on jak zwykły pendrive, który możemy włożyć do naszego portu USB w komputerze lub w niektórych telefonach. Są też klucze U2F, które potrafią bezprzewodowo połączyć się z naszym smartfonem dzięki technologii NFC. Być może wszystko to brzmi trochę skomplikowanie, ale tak naprawdę w użyciu jest bardzo proste. Gdy mamy taki klucz skonfigurowany i podpięty do naszej poczty e-mail czy innego serwisu to po prostu przy logowaniu wkładamy ten klucz do portu USB (lub przykładamy do smartfona), dotykamy go palcem i możemy się bezpiecznie logować.

Dlaczego jest to bezpieczne? Ponieważ ten klucz sprawdza za nas, czy strona do której się logujemy jest stroną prawdziwą, czyli bezpieczną. Dzięki temu kluczowi jesteśmy w stanie zabezpieczyć nasze skrzynki e-mail, konto Google czy konto na YouTube. Niestety jak na razie nie ma jeszcze możliwości zabezpieczyć w ten sposób konta bankowego.

Jak bezpiecznie płacić przez Internet?

A jak to jest z płatnościami w Internecie? Czy istnieje bezpieczna forma zakupów przez internet? Tak. Okazuje się, że najbezpieczniejszą formą płatności bezgotówkowych, czy to w Internecie czy fizycznie w sklepie, jest płatność kartą, zwykłą lub kredytową. Karty płatnicze mają mechanizm chargeback, który daje możliwość użytkownikowi reklamowania każdej transakcji dokonanej kartą. Dzięki temu, jeżeli nawet wejdziemy na stronę oszusta i wpiszemy tam dane naszej karty, przez co stracimy jakąś kwotę z tej karty, to zgłaszając reklamacje praktycznie na 100% te pieniądze odzyskamy. Nawet jeżeli przy pomocy karty kupimy coś przez Internet i przyjdzie do nas rzecz niezgodna z opisem, a sprzedający nie będzie chciał uznać reklamacji, wówczas zgłaszamy to do naszego banku i bank po wyjaśnieniu sytuacji zwróci nam nasze pieniądze. Płacąc za usługi kartą macie Państwo możliwość odzyskania pieniędzy nawet jeżeli zapłacicie jakiejś firmie, która w między czasie zbankrutuje i przez to nie wykona usługi za którą zapłaciliście lub nie dostarczy produktu. Nawet wówczas również możecie odzyskać swoje środki. Tak więc płatność kartą jest naprawdę bezpieczna.

WARTO WIEDZIEĆ

Kwestia bezpieczeństwa w Internecie jest tak szeroka, że nie sposób omówić ją w całości w jednym skrypcie. Dlatego też na zakończenie odsyłam Państwa do trzech stron, które specjalizują się w tym temacie, a znajdziecie tam Państwo mnóstwo niezwykle przydatnych treści odnośnie bezpieczeństwa w sieci. Nasza fundacja nie ma żadnych korzyści z polecania tych firm, a robimy to dlatego, że umieszczane przez ich twórców darmowe informacje mogą uchronić Państwa przed stratą pieniędzy, danych czy po prostu niepotrzebnym stresem. Strony te to:

www.niebezpiecznik.pl

www.sekurak.pl

www.zaufanatrzeciastrona.pl

Fundacja "Idea dla Ciebie"
Ignaców 14a
63-507 Kobyla Góra
tel. 695919344
www.ideadlaciebie.org