Grupa GPEC

PORADNIK BEZPIECZEŃSTWA

ZAGROŻENIA CYBERPRZESTRZENI I JAK DBAĆ O BEZPIECZEŃSTWO

ZAGROŻENIA CYBERPRZESTRZENI

I. Phishing

Spam bywa groźny: mogą pojawiać się w nim wiadomości od przestępców, którzy próbują wydobyć poufne informacje. Podszywają się np. pod dostawcę usług i nakłaniają, aby zainstalować program z wirusem lub oprogramowanie szpiegujące. Dzięki phishingowi przestępcy mogą wyłudzić Państwa poufne dane lub zainfekować Państwa urządzenie. Przestępcy tworzą fałszywe strony internetowe. Podszywają się pod instytucje zaufania publicznego i zachęcają, aby wejść na tę stronę. Przestępcy wysyłają maile, których tytuł lub treść ma spowodować otwarcie przez Państwa linka lub załącznika. Bardzo często takie wiadomości zawierają informację o zablokowanym koncie, dodatkowej weryfikacji danych lub niezapłaconej fakturze.

Popularny jest phishing na portalach społecznościowych i komunikatorach.

Oszuści mogą napisać do Państwa wiadomość z konta Państwa znajomego po przejęciu nad nim kontroli. W rozmowie poproszą o pomoc i przelew pieniędzy. Jeśli klikną Państwo w podany przez nich link i wpiszą swoje dane, narażają się na przejęcie Państwa danych lub kradzież.
Innym sposobem jest promocja fałszywej strony w wyszukiwarce. Fałszywa strona jest najczęściej łudząco podobna do prawdziwej strony.
Aby Państwa zmylić, w adresie takiej strony oszuści często podają nazwę prawdziwej instytucji, pod którą się podszywają.

II. Złośliwe oprogramowanie

Złośliwe oprogramowanie (np. wirus komputerowy) to kod, który nie może działać sam. Potrzebuje programu komputerowego. Jeśli ściągną Państwo taki program i go uruchomią, to włączą Państwo także wirusa.

Wirus może działać na różne sposoby:

- **wyłudzi dane**
- **ukradnie tożsamość**
- **zainfekuje pliki, gdy będą tworzone lub uruchamiane**
- **skasuje lub uszkodzi dane w systemach i plikach**
- **ukradnie dane, którymi logują się Państwo do portali społecznościowych i kont pocztowych**

III. Wykorzystanie luk w oprogramowaniu

Przestępcy wyszukują luki w kodzie programów i bezwzględnie je wykorzystują. Gdy uzyskają dostęp do komputera, mogą zainstalować szkodliwe oprogramowanie, które zmienia działanie komputera lub urządzenia mobilnego.
Tworzone jest złośliwe oprogramowanie, następnie przesyłane poprzez maile, które mają przykuć Państwa uwagę i skłonić, aby otworzyli Państwo link lub załącznik. Bardzo często takie wiadomości dotyczą zablokowanego konta, dodatkowej weryfikacji urządzenia lub niezapłaconej faktury.
Przestępcy mogą też zainfekować smartfon. Zwłaszcza przy pobraniu oprogramowania przez link z SMS-a od nieznanego nadawcy.
Przestępcy umieszczają też złośliwe aplikacje w sklepach internetowych. Często podszywają się pod inne aplikacje. Takie aplikacje będą często wymagać dostępu do naszych SMS-ów.

IV. Fałszywe faktury

Przestępcy wysyłają podrobioną fakturę ze zmienionym numerem rachunku. Faktura może przyjść z adresu mailowego kontrahenta, jeśli przestępcy przełamią zabezpieczenia na jego komputerze.
Złośliwe oprogramowanie może wysyłać wiadomości poza kontrolą właściciela skrzynki mailowej.

Jeśli mają Państwo wątpliwości, należy zadzwonić do kontrahenta i upewnić się, że wysłał do Państwa fakturę.

V. Fałszywe komunikaty na stronie lub w serwisie

Przestępcy mogą wyświetlać fałszywe treści nawet podczas połączenia przez stronę kontrahenta lub instytucji. Mogą to zrobić, jeśli Państwa komputer jest zainfekowany. Spróbują wtedy wyłudzić poufne dane SMS.

Jeśli mają Państwo zainfekowany telefon, przestępcy mogą też wyświetlać fałszywe treści, gdy uruchamiasz aplikację. Będą próbowali wyłudzić Państwa dane, a także odbierać i wysyłać wiadomości SMS.

VI. Fałszywe sklepy i oferty

Przestępcy tworzą fałszywe sklepy internetowe, oferując towar w atrakcyjnych cenach. Pomimo zapłacenia za zakupy w takim sklepie przesyłka może nigdy do Państwa nie dotrzeć.

Przed zakupem należy sprawdzić od kogo dokonywany jest zakup towaru:

jak długo istnieje dana firma

czy można się do niej dodzwonić

czy otrzymają Państwo odpowiedź na maila

Przestępcy mogą także wystawić towar na portalu ogłoszeniowym „za darmo" - w zamian za opłacenie przesyłki. Nabywcy podsyłają link do szybkich przelewów, czyli do fałszywej strony. Przechwytują Państwa dane do logowania, definiują nowego odbiorcę lub zmieniają wysokość przelewu.

JAK DBAĆ O BEZPIECZEŃSTWO?

I. Bezpieczne urządzenia

Z serwisów transakcyjnych należy korzystać tylko na sprawdzonych urządzeniach.
Należy unikać logowania do aplikacji i stron z cudzych komputerów i urządzeń mobilnych.

Należy regularnie aktualizować system operacyjny na komputerze.

Aplikacje i programy należy pobierać wyłącznie z oficjalnych źródeł.

Należy korzystać z dodatkowych programów (np. antywirus, firewall), które chronią komputery i urządzenia mobilne

Nie należy zmieniać ustawień bezpieczeństwa urządzenia, a w szczególności nie należy usuwać ograniczeń, które narzucił producent.

Należy blokować ekran urządzenia za pomocą dodatkowego zabezpieczenia (np. hasło, PIN).

1. Urządzenia mobilne

Smartfony i tablety coraz częściej zastępują inne urządzenia osobiste. Podobnie jak komputery, urządzenia mobilne wymagają odpowiedniej ochrony przed wirusami.

Wielu użytkowników, myśląc o bezpieczeństwie telefonu lub tabletu, obawia się, że go zgubi, lub ktoś go ukradnie. Tymczasem bardziej powinniśmy się obawiać, że ktoś przejmie nad nim kontrolę.

O czym pamiętać, żeby bezpiecznie korzystać z aplikacji na urządzeniu mobilnym?

- Należy używać oprogramowania antywirusowego
- Należy blokować ekran hasłem lub PIN-em
- Należy instalować aktualizacje aplikacji i systemu operacyjnego
- Należy pobierać i instalować aplikacje wyłącznie z oficjalnych sklepów z aplikacjami
- Nie należy uruchamiać linków z wiadomości SMS lub e-mail, jeśli istnieje wątpliwość, że pochodzą z niebezpiecznego i niezaufanego źródła
- Nie należy łączyć aplikacji mobilnej ze swoim kontem na obcych urządzeniach
- Nie należy odczytywać kodów QR nieznanego pochodzenia
- Należy ostrożnie podchodzić do instalacji aplikacji, które wymagają uprawnień do odczytywania i wysyłania wiadomości SMS
- Jeśli nie korzystają Państwo w danej chwili z Wi-Fi lub Bluetooth, należy je wyłączyć

Uwaga!

Żadna instytucja nigdy nie prosi, abyś instalował dodatkowe aplikacje lub certyfikaty.

2. Komputer

Bezpieczny komputer powinien mieć:

- Aktualizowany i legalny system operacyjny
- Oprogramowanie typu firewall

  Firewall (zapora sieciowa) to jeden ze sposobów zabezpieczania komputerów, sieci i serwerów przed intruzami. Firewall stał się nieodzownym oprogramowaniem każdego komputera podłączonego do sieci.

  Zapora na domowym komputerze sprawdza cały ruch w sieci oraz ogranicza dostęp nieznanym programom lub użytkownikom.

- Oprogramowanie antywirusowe zabezpieczające przed spyware i adware

  To oprogramowanie, które wykrywa, zabezpiecza, zwalcza, usuwa i naprawia szkody, które powodują wirusy. Jeśli aplikacja zawiera szkodliwe oprogramowanie, program antywirusowy wykonuje odpowiedni ruch, który wyklucza wirusa i pozwala na bezpieczny dostęp do uruchamianego programu. Ważne jest, aby każdego antywirusa odpowiednio często aktualizować. Pozwala mu to „być na bieżąco" w świecie wirusów.

  Dzięki aktualizacji program zbiera informacje o najnowszych wirusach i dostaje instrukcje, które pozwalają mu je zwalczać i naprawiać. Cenione na rynku firmy, które produkują oprogramowanie antywirusowe, codziennie aktualizują definicje wirusów.

- Oprogramowanie antyspamowe

  To rodzaj oprogramowania, które blokuje niechcianą korespondencję mailową. Programy filtrują wiadomości i wykorzystują tak zwane czarne listy adresów i domen używanych przez spamerów. W większości tego typu oprogramowań możemy zmieniać ustawienia reguł (np. określać słowa klucze występujące w materiałach reklamowych). Pozwala to zablokować naszą skrzynkę pocztową na wiadomości, które zawierają te słowa w tytule przesyłki.

  Jednak programy te nie są bezbłędne i potrafią czasem zablokować korespondencję, która powinna być dostarczona, dlatego warto sprawdzać folder spam i weryfikować, czy wszystkie wiadomości, które do niego trafiły, rzeczywiście powinny się w nim znaleźć.

II. Bezpieczne hasła

Należy stosować skomplikowane hasła i zadbać o to, aby trudno było je odgadnąć.

Minimum osiem znaków, w tym znaki specjalne, liczby, duże i małe litery.

Nie należy używać w haśle trywialnych zwrotów oraz informacji, które łatwo z Tobą powiązać (np. imię czy nazwisko) lub odgadnąć (np. aktualny miesiąc, rok).

Należy regularnie zmieniać hasła i nie udostępniać ich nikomu.

Należy używać unikalnych haseł do serwisów www. Nie należy wykorzystywać tych samych haseł, które stosuje się w innych systemach, na forach czy portalach.

III. Bezpieczne logowanie do e-BOK

- Nigdy nie należy udostępniać osobom trzecim identyfikatora (loginu) ani hasła dostępu. Hasło do logowania w serwisie ustalają Państwo samodzielnie
- Wpisując identyfikator (login) i hasło należy się upewnić, że nikt ich nie podpatruje
- Nie należy logować się do aplikacji na komputerach dostępnych w miejscach publicznych
- Należy stosować bezpieczne hasła i starać się nie używać prostych do odgadnięcia haseł
- Nie należy zapisywać nigdzie haseł i pamiętać o ich regularnej zmianie
- Nie należy odchodzić od komputera, jeżeli jesteś zalogowany. Należy się wylogować i zamknąć przeglądarkę
- Należy sprawdzać datę ostatniego poprawnego oraz niepoprawnego logowania
- Jeśli na stronie logowania pojawią się dodatkowe pola, które należy uzupełnić np. wpisać dane osobowe lub hasło jednorazowe, lub zauważą Państwo jakiekolwiek nieprawidłowości, nie należy podawać danych i natychmiast zgłosić problem do Biura Obsługi Klienta.

IV. Bezpieczna instalacja aplikacji

Aplikacje powinny być pobierane z autoryzowanych sklepów:

App Store	Google Play	Windows Phone Store	Windows Store
(iOS - Apple)	(Android)	(Windows Phone)	(Windows 8.1)

Należy korzystać tylko z tych sklepów, ponieważ znajdujące się tam programy są cyfrowo podpisane i są sprawdzane pod kątem bezpieczeństwa.

Nigdy nie należy pobierać aplikacji z niezaufanych źródeł oraz należy unikać pobierania aplikacji od osób trzecich.

Należy ostrożnie podchodzić do instalowania aplikacji, które żądają od Państwa nadania uprawnień do odczytywania lub wysyłania wiadomości SMS.

V. Bezpieczne maile

- Nie należy otwierać podejrzanych maili i załączników
- Należy zwracać szczególną uwagę na załączniki posiadające kilka rozszerzeń plików jednocześnie, np. przelew.pdf.zip, wyplata.jar.doc
- Należy sprawdzać, czy rzeczywisty adres odnośnika (link) jest spójny z tym, który widzą Państwo w treści maila
- Należy zwrócić uwagę na wiarygodność nadawcy oraz sposób, w jaki zwraca się do Państwa
- Nigdy nie należy logować się do serwisu transakcyjnego z linka, który otrzymali Państwo w mailu
- Nie należy realizować transakcji na podstawie maila. Należy sprawdzić dokładnie tego typu dyspozycje

VI. Bezpieczne strony www

- Należy sprawdzić poprawność witryny serwisu www, z którym się Państwo łączą (certyfikat oraz połączenie HTTPS)
- Nie należy wchodzić na podejrzane i nieznane witryny

  Należy zwracać uwagę na adresy URL stron, które Państwo odwiedzają, zwłaszcza na tzw. skrócone adresy URL. Takie strony mogą zainfekować Państwa urządzenie złośliwym oprogramowaniem
- Nie należy podawać danych osobowych na niezaufanych witrynach, w szczególności loginu i hasła na stronach obcych serwisów
- Logując się do serwisów, należy wpisywać stronę logowania samodzielnie lub używać przycisku „Zaloguj" po ręcznym wpisaniu adresu strony

  Nie wolno korzystać z linków do logowania, które otrzymują Państwo mailem czy w portalach społecznościowych

  Nie powinno się szukać strony do logowania w wyszukiwarce internetowej – można trafić na fałszywe strony, które udają stronę, na którą chcą się Państwo zalogować

VII. Bezpieczne profile i oferty

Jeżeli dostali Państwo prośbę od znajomego, aby zrobić mu przelew uważaj – możliwe, że piszesz z oszustem. Należy skontaktować się ze znajomym w inny sposób i potwierdzić, że faktycznie to on prosi Państwa o przelew.

Przed zakupem należy sprawdzić, od kogo kupuje się towar: jak długo istnieje dana firma, gdzie ma siedzibę, czy można się do niej dodzwonić oraz jakie opinie wystawili inni kupujący.

Nie należy ufać ofertom pracy, które przychodzą bezpośrednio na Państwa skrzynkę pocztową, szczególnie tym wyjątkowo atrakcyjnym. Gdy szukają Państwo pracy, należy korzystać wyłącznie ze znanych portali.

VIII. Bezpieczne rozmowy telefoniczne

- Nie należy ujawniać prywatnych danych, dopóki nie ma się pewności, z kim się rozmawia. Pracownika instytucji zawsze można sprawdzić oddzwaniając do Biura Obsługi Klienta i potwierdzając jego tożsamość
- Nie należy ufać nieznanemu rozmówcy, który chce, aby podać mu poufne dane (hasła, PIN-y)