KPP KOŃSKIE

https://konskie.swietokrzyska.policja.gov.pl/tkn/dzialania-policji/aktualnosci/22682,Jak-bezpiecznie-korzystac-z-Internetu.html
2020-10-31, 02:27

JAK BEZPIECZNIE KORZYSTAĆ Z INTERNETU

Internet, to nie tylko źródło informacji czy sposób na załatwienie ważnych dla nas spraw. Niestety niesie on ze sobą wiele pułapek, a nasza niewiedza dotycząca metod, jakimi posługują się Internetowi przestępcy, może nas kosztować utratę danych lub pieniędzy, czy też narazić na niebezpieczeństwo nas lub naszych najbliższych.

Jedną z metod jakimi posługują się przestępcy działający w sieci jest phishing. Phisher przeważnie rozpoczyna atak od rozesłania pocztą elektroniczną odpowiednio przygotowanych wiadomości, które udają oficjalną korespondencję z banku, serwisu aukcyjnego lub innych portali. Zazwyczaj zawierają one informację o rzekomym zdezaktywowaniu konta i konieczności jego ponownego reaktywowania. W mailu znajduje się odnośnik do strony, na której można dokonać ponownej aktywacji konta. Pomimo że witryna z wyglądu przypomina stronę prawdziwą, w rzeczywistości jest to przygotowana przez przestępcę pułapka. Nieostrożni i nieświadomi użytkownicy ujawniają swoje dane uwierzytelniające (kody pin, identyfikatory i hasła). Bywa również, że przestępcy posługują się prostszymi metodami, które polegają na wysłaniu maila z prośbą, czasem wręcz żądaniem, podania danych służących do logowania na konto i jego autoryzacji.

„Robaki” i pharming

Innym sposobem działania cyberprzestępców, który ma doprowadzić do poznania poufnych danych, jest wykorzystywanie złośliwego oprogramowania, zwanego w zależności od swojej formy: robakami, koniami trojańskimi (trojanami) lub wirusami. Takiego "robaka" można ściągnąć korzystając z zainfekowanych witryn internetowych.

Bardziej zaawansowaną, a co za tym idzie niebezpieczniejszą dla użytkownika oraz trudniejszą do wykrycia formą phishingu jest tzw. pharming. Zamiast wysyłania fałszywych wiadomości e-mail, przestępcy przekierowują użytkowników wpisujących prawidłowe adresy np. swojego banku, na fałszywe strony internetowe.

Każdy internauta powinien mieć świadomość zagrożeń, jakie wiążą się z pobieraniem z sieci oprogramowania z niepewnych serwerów czy odpowiadaniem na podejrzaną pocztę elektroniczną. Pamiętajmy, że:

serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie;
nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila;
należy regularnie uaktualniać system i oprogramowanie;
nie wolno przesyłać mailem żadnych danych osobistych - w żadnym wypadku nie wypełniajmy danymi osobistymi formularzy zawartych w wiadomości e-mail;
zastanówmy się nad napisaniem wiadomości e-mail zwykłym tekstem zamiast HTML;
banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Adres strony WWW rozpoczyna się wtedy od wyrażenia 'https://', a nie 'http://'. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych;
każde podejrzenia co do sfingowanych witryn należy jak najszybciej przekazać policjantom lub pracownikom danego banku odpowiedzialnym za jego funkcjonowanie w sieci.

Pamiętajmy również, że czasem niewiele potrzeba, aby zmniejszyć ryzyko utraty danych i ich poufności. Wystarczy

ograniczać fizyczny dostęp do komputerów, oprogramowania i nośników danych osobom trzecim. Warto również regularnie zabezpieczać dane wykonując kopie bezpieczeństwa i aktualizować na bieżąco programy antywirusowe, „ściany ogniowe" oraz używać oprogramowania z wiadomych i sprawdzonych źródeł.

Zahasłuj swoje hasło

Jedną z podstawowych zasad jakich należy przestrzegać, aby zabezpieczyć swoje dane jest używanie jakościowych haseł (składających się z małych i wielkich liter, cyfr i znaków specjalnych, o długości powyżej 8 – 10 znaków)! Nie należy stosować haseł domyślnych, ani posługiwać się jednym hasłem do wielu programów i portali. Warto również zmieniać je co pewien czas, zwłaszcza po wykryciu przez program antywirusowy złośliwego oprogramowania. Nie należy zapisywać haseł i pinów w nieszyfrowanych plikach tekstowych na twardym dysku.

Aby uchronić się przed niebezpieczeństwami płynącymi z sieci:

jeżeli korzystamy w domu z sieci bezprzewodowej (WiFi) odpowiednio skonfigurujmy router. Hasła zabezpieczające należy tworzyć, używając cyfr, małych i dużych liter oraz znaków specjalnych. Przy wyborze kupna routera sugerujmy się nie tyle ceną, co możliwością szyfrowania WPA czy WPA2,
używajmy programów antywirusowych, które uchronią nas przed niepożądanymi wirusami i innymi niebezpieczeństwami. Nie zapomnijmy o systematycznej aktualizacji,
uważajmy na e-maile niewiadomego pochodzenia, które zawierają podejrzane załączniki, nigdy ich nie otwierajmy,
nie odpisujmy na spamy, ponieważ nasz e-mail zostanie uznany za aktywny i będą do nas przysyłane kolejne wiadomości z podejrzana treścią.

Bezpieczne zakupy w Internecie

Coraz częściej robimy zakupy korzystając z popularnych portalami aukcyjno-ogłoszeniowych. Wiele osób zgłasza się na Policję, aby poinformować o oszustwie. Zdarza się, że poszkodowani zamiast zamówionego towaru otrzymują bezwartościowe przedmioty tj. kamienie, stare gazety, bądź przesyłka w ogóle do nich nie dociera. Zapłacenie za przedmiot i nie otrzymanie go to nic innego jak wyłudzenie czyli oszustwo. Kodeks Karny przewiduje za ten czyn karę nawet do 8 lat pozbawienia wolności.

Aby zakupy przez Internet były bezpieczne wystarczy przestrzegać podstawowych zasad i zwracać uwagę na kilka szczegółów. Przede wszystkim zwracajmy uwagę, na cenę produktu – bardzo tani, powinien od razu obudzić naszą czujność. Czytajmy komentarze na temat sprzedającego – duża ilość tych pozytywnych, to mniejsze ryzyko. Ważne jest także to, od kiedy sprzedawca jest zalogowany w serwisie i ile osób korzystało z jego usług.

Nie zapominajmy również o dokładnym przeczytaniu opisu aukcji i regulaminu zakupu. W razie jakichkolwiek wątpliwości pytajmy sprzedawcę telefonicznie lub mailowo. Jeśli sprzedającym jest firma warto sprawdzić, czy rzeczywiście ona istnieje. Potwierdzajmy wygranie licytacji, ale z wpłatą pieniędzy poczekajmy kilka dni, żeby upewnić się czy wszystko jest w porządku. Opóźni to czas dostawy, ale w przypadku gdy konto zostało przejęte przez osobę podszywającą się, zmniejszamy ryzyko. W ciągu tych kilku dni prawdziwy właściciel zorientuje się i powiadomi portal aukcyjny, a oni nas. Koniecznie gromadźmy też całą korespondencję ze sprzedającym. Nie zajmuje wiele miejsca, a jest bezcennym dowodem kontaktów ze sprzedającym.

Dziecko w sieci

Mówiąc o bezpiecznym Internecie nie możemy zapominać o dzieciach i młodzieży korzystających z sieci. Często przeglądane przez młodych ludzi treści są nieadekwatne do ich wieku, a co więcej mogą wpływać niekorzystnie na ich psychikę i zachowanie. Ważną rolę w procesie uświadamiania najmłodszych odgrywają rodzice. To oni, jako pierwsi powinni poinformować swoje pociechy o możliwych zagrożeniach.

Rady dla rodziców:

rozmawiajmy ze swoimi dziećmi, omawiajmy kwestie bezpiecznego korzystania z komputera i Internetu,
kontrolujmy, co nasze dzieci robią w sieci, na jakie strony zaglądają, jakich szukają informacji
w przypadku napotkania w Internecie nielegalnych treści nie zastanawiajmy się i zgłośmy ten fakt na Policję,
zapytajmy informatyka o możliwości blokady niektórych stron.

Często rodziców nurtuje pytanie:„co powiedzieć dzieciom, na co powinny uważać, do kogo mają zwrócić się o pomoc, w przypadku problemów w sieci”. Odpowiedz jest prosta. Oto kilka rad przygotowanych dla dzieci:

pamiętaj, że przyjaciele poznani w Internecie mogą nie być tymi, za których się podają – w rzeczywistości możesz rozmawiać z osobą, która ma wobec ciebie złe zamiary,
nie podawaj w Internecie swojego nazwiska, wieku, numeru telefonu – najlepiej jest posiadać swój nick, internetową ksywkę,
nie umawiaj się z osobami poznanymi przez Internet,
uważaj na e-maile otrzymane od nieznajomych, nigdy nie otwieraj podejrzanych załączników i nie otwieraj linków przesłanych ci przez nieznaną osobę – mogą zawierać wirusy,
traktuj innych z szacunkiem, nie wyzywaj, nie strasz, nie obrażaj,
rozmawiaj z rodzicami o Internecie, zaproś ich na twoje ulubione strony, pokaż im jak szukać w Internecie informacji – zostań ich nauczycielem,
w razie zagrożenia szukaj pomocy u dorosłych – rodziców, pedagoga, policjanta.

Bez względu na to ile mamy lat korzystając z sieci, nie zapominajmy nigdy o przestrzeganiu zasad bezpieczeństwa. Warto wiedzieć co robić, a czego nie, aby nie paść ofiarą oszustów czy hakerów.

Źródło: KGP