Komenda Wojewódzka Policji

w Bydgoszczy

Zagrożenia w sieci Internet

jak je rozpoznawać i jak się chronić.

Część I

Wstęp

Krótki podstawowy poradnik dla użytkowników komputerów i urządzeń z dostępem do Internetu.

Poradnik został opracowany dla osób, które często korzystają z Internetu, ale ich wiedza o bezpieczeństwie jest niska i dodatkowo nie potrafią rozpoznawać zagrożeń.

Ujęte tematy przedstawione są w sposób prosty, krótki a zarazem możliwie jasny, aby każdy użytkownik po tej lekturze mógł rozpoznać zagrożenia i się przed nimi chronić.

(źródło grafiki – www.gov.pl)

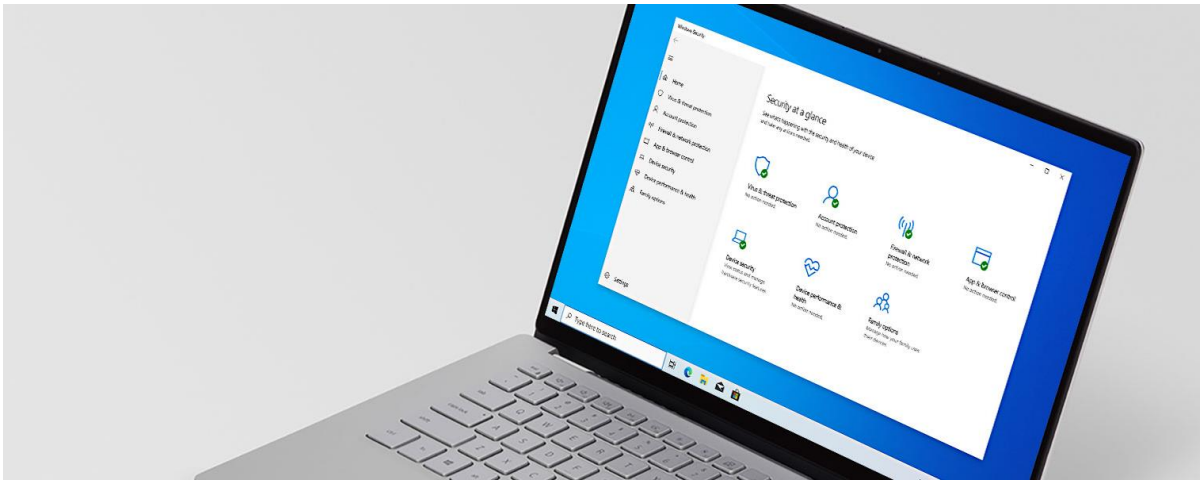
1. Phishing – co to jest?

Jest to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji takich jak:
- danych logowania (login, hasło) do poczty elektronicznej, serwisów społecznościowych itp.
- danych karty kredytowej/płatniczej
- zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań np. instalacja oprogramowania na naszym komputerze, telefonie, tablecie.

Sprawcy działają poprzez:
1. **SMS** – np. z zaległymi płatnościami o niskich kwotach, informacjami o naruszeniu bezpieczeństwa w banku itp.
2. **połączenie telefoniczne** – podszywanie się pod pracownika banku, jednocześnie podszywając się pod prawdziwy numer naszego banku.
3. **wiadomość email** – weryfikacja konta w wyniku rzekomego naruszenia bezpieczeństwa z prośbą o autoryzację klikając w link.
- Tytułowanie wiadomości z dopiskiem „Re” sugerując, że to my do nich pierwsi pisaliśmy.
- Podszywanie się pod dyskonty spożywcze np. Biedronka, Lidl, Żabka lub podszywanie się pod firmę kurierską, instytucję itp.
- podszywanie się pod duże firmy odzieżowe, sportowe oferujące konkursy z super nagrodami, rabatami itp. W rzeczywistości chodzi o pozyskanie naszych danych osobowych.
4. **reklamy** – oferty szybkiego zarobku np. w kryptowalucie, super diety, specyfiki lecznicze itp. Często takie oferty na swojej stronie posiadają pozytywne opinie rzekomo powiązane z Facebook, dodane przed chwilą, które w rzeczywistości są nieprawdziwe a mają w nas wzbudzić zaufanie.
5. **fałszywe strony -** Sprawcy wykorzystują podobieństwo w wyglądzie liter/cyfr/znaków.
Przykład?
„rn” - „m”
„q” - „g”

„vv” - „w”
„l” (małe „L”) jak „l” (duże „i”)
„i” – „í”(litera języka obcego)
pkobp.pl czy **pkobp.pl** (w rzeczywistości to adres - xn--pkbp-65d.pl)
bgz.pl czy **bgz.pl** (w rzeczywistości to adres **-** xn--bz-jgb.pl)

6. **konkursy** – testowanie produktu za darmo (oferowane np. na Facebooku). Często są to prawdziwe konkursy, gdzie prawdziwa jest nagroda, lecz „haczyk” polega na tym, że konkurs trwa np. przez 6 miesięcy w czasie którego zbierane są zapisy na testowanie produktu. Należy tylko podać swoje pełne dane osobowe i wyrazić wszystkie zgody marketingowe. Przez te 6 miesięcy wyłoniona zostanie tylko 1 osoba, która otrzyma nagrodę, a zebrane dane osobowe posłużą do dalszej sprzedaży podmiotom zewnętrznym co wyraźnie jest określone w regulaminie konkursu (niestety, nikt go nie czyta). Następnie nasze dane są wykorzystywane do telemarketingu itp.
7. **ogłoszenia** – sprzedaż „niedostępnych” produktów. Sprawcy często wykorzystują fakt pojawienia się nowości elektronicznych na rynku, których dostęp jest ograniczony np. konsoli PlayStation i wystawiają ogłoszenia z atrakcyjną ceną po to aby nas skusić na zakup towaru, lecz nigdy nie otrzymamy.
8. **portale ogłoszeniowe** – podszywanie się pod kupującego i przesłanie podrobionego linku do płatności. - Dość często spotykane. N/n osoba kontaktująca się przez komunikator WhatsApp pytając się o nasz produkt prowadzi z nami korespondencję i prosi nas o dane numeru konta bankowego, Paypal, adres email, dane adresowe. Przedstawia się jako osoba przebywająca za granicą, ale jego znajomy odbierze od nas towar za, który chce zapłacić z góry. Oczywiście to oszustwo.
9. **Fałszywe informacje** – chodzi oczywiście o informacje np. „o rzekomej śmierci po szczepieniu”, „o tragicznym wypadku – prawdziwe zdjęcia”, „ o odnalezionym porwanym dziecku”.
Oczywiście chodzi o to, aby zobaczyć informację, musimy się zalogować do Facebooka podając login i hasło na fałszywej stronie.



(źródło grafiki – www.microsoft.com)

2. Antywirus – czy potrzebny?

Jak wiadomo, system operacyjny Windows 10 posiada już wbudowany program antywirusowy Defender oraz Firewall, co oznacza, że nasz komputer jest chroniony.
No tak, tylko czy tak jest w rzeczywistości?.

I TAK i NIE!

TAK – bo jest wystarczający i wystarczająco dobry,

NIE – ponieważ, po pierwsze - aby był w pełni skuteczny, trzeba go poprawnie skonfigurować, a tu jest potrzeba wiedza informatyczna.

Po drugie, on nie chroni nas tak jak programy zewnętrzne płatne.

Dlaczego?

Ponieważ programy zewnętrzne oferują nam dodatkowe usługi ochrony naszego komputera, takie jak:

- dodatkowy tzw. „pakiet internetowy”,
- analiza aktualizacji zainstalowanych programów i ewentualna ich aktualizacja,
- czyszczenie komputera ze śmieci,
- menager haseł, który tworzy skomplikowane hasła i je dla nas bezpieczne zapamiętuje,
- chroni/ostrzega nas przed podejrzanymi, niebezpiecznymi stronami internetowymi,
- chroni przed ransomware*,

* *Ransomware – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego*.

- chroni przed malwarem*

* *Malware - uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika.*

- ochrona przed komputerem ZOMBI,
- ochrona rodzicielska, która pozwala zarządzać komputerem przez rodzica i chroni przed zakazanymi treściami.

(źródło grafiki – www.komputerswiat.pl)

3. Komputery ZOMBI

Komputer ZOMBI – boty

Autorzy botów przejmują kontrolę nad naszym pecetem i z premedytacją używają go do popełniania przestępstw w Internecie. Opanowane w ten sposób komputery w żargonie fachowym określane są jako zombi - tak samo, jak na wpół martwe istoty z horrorów, które pozbawione własnej woli stają się ślepymi wykonawcami rozkazów. Szczególna perfidia procederu polega na tym, że niczego nieprzeczuwający właściciel takiego „zombi" nieświadomie staje się sprawcą przestępstw: boty służą nie tylko do wykradania danych osobistych, ale również do przeprowadzania ataków na osoby trzecie np. DDoS lub ukrywania się w sieci.

Niestety, jak wynika z doświadczenia dość często można spotkać się z takimi komputerami co jest niepokojące, a użytkownicy nieświadomi.

4. Jak się chronić?

Z doświadczenia wynika, że duża ilość użytkowników Internetu bagatelizuje bezpieczeństwo w tym:
- nie aktualizuje systemu,
- wyłącza zabezpieczenia w komputerze,
- nie używa żadnego programu antywirusowego, nawet darmowego.

Co należy robić?

Najważniejsze czynności:

- włączyć podwójne uwierzytelnianie (uwierzytelnianie dwuskładnikowe) na portalach – Facebook, Allegro, konto Google w tym poczta, konta Bankowe, pocztowe i inne wszystkie oferujące taką funkcje,
- instalować oprogramowanie z legalnego źródła,
- dokładnie sprawdzać linki do stron,

- nie klikać w otrzymane złączniki przesłane poprzez sms, email, przede wszystkim z dziwnych adresów lub ukrytych adresów,
- jeżeli masz jakieś wątpliwości, możesz wejść na prawdziwą stronę np. banku, operatora telefonii komórkowej , sklepu internetowego, urzędu lub po prostu zadzwonić i potwierdzić,
- instalować aktualny antywirus – najlepiej licencjonowany z firewall (koszt to już ok 40 zł rocznie za jedno stanowisko),
- regularnie aktualizować system, przeglądarekę,
- profilaktyka – nie instalować niczego na próbę bez sprawdzenia co to jest – „wujek google” oraz „ciocia Wikipedia” powie nam co to jest i jakie niesie za sobą zagrożenia,
- przy instalacji programu czytać jakie zgody wyrażamy,
- czytać regulaminy stron oferujące konkursy itp.,
- zachować zdrowy rozsądek,
- „Czyścić” komputer programami – antywirus, antymalware np. darmowy AdwCleaner

Sprawdź swój adres email na stronie internetowej:

http://haveibeenpwnd.com, czy aby już nie krąży gdzieś w sieci jako „skompromitowany”.

*(zrzuty ekranowe w tłumaczeniu translatorowym)

Jeżeli twój adres email pokaże się jako czerwony, nie panikuj, tylko zmień hasło na nowe bezpieczne składające się z małych i dużych liter, cyfr i znaku specjalnego.

Opracował:

asp. szt. Marcin Matysek
Wydział dw. z Cyberprzestępczością
Komendy Wojewódzkiej Policji
w Bydgoszczy