edukacja medialna

Phishing i spam

WIEDZA W PIGUŁCE

Phishing i spam to dwie różne metody osiągnięcia zysku naszym kosztem.

Phishing jest rzadszym, ale znacznie groźniejszym zjawiskiem, w którym atakujący usiłuje przejąć naszą tożsamość, aby uzyskać jakąś korzyść. Najczęściej skuteczny atak phishingowy oznacza, że przestępca odchodzi z pieniędzmi, a my zostajemy z długami i koniecznością udowadniania, że jesteśmy ofiarami, a nie sprawcami.

Podstawową zasadą ochrony przed phishingiem jest ochrona danych wrażliwych, do których należą wszystkie dane osobowe: imię i nazwisko, adres, itp. Szczególnie chronić należy datę i miejsce urodzenia oraz nazwisko panieńskie matki, gdyż te dane służą najczęściej do weryfikacji tożsamości w bankach przy kontaktach przez telefon.

Nigdy też nie należy podawać nikomu numeru naszego konta bankowego czy karty. Hasła i kody do kont pocztowych lub serwisów społecznościowych również powinny być ścisłą tajemnicą.

Choć zasady te brzmią prosto i rozsądnie, to atakujący różnymi metodami starają się skłonić nas do ujawnienia tych informacji. Czasami jest to telefon, w którym nieznana ci osoba prosi o podanie hasła do emaila w jakiejś nie cierpiącej zwłoki sprawie służbowej. Innym razem jest to email, w którym bank albo serwis aukcyjny prosi o podanie hasła w celu „weryfikacji tożsamości". Osoby nieobeznane z procedurami bezpieczeństwa obowiązującymi w takich firmach często padają ofiarą całkiem prostych tricków socjotechnicznych. Bywa jednak, że atakujący naszą tożsamość budują skomplikowane, rozbudowane strony internetowe łudząco podobne do autentycznych lub poświęcają na zdobycie potrzebnych im informacji dużo czasu, rozbudowując swoją opowieść i zdobywając nasze zaufanie. Jedynym rozwiązaniem jest kategoryczna wierność zasadzie ochrony danych wrażliwych.

Bardzo ważne jest też zabezpieczenie naszych urządzeń przed nieuprawnionym dostępem, ochrona dostępu hasłem, szyfrowanie pamięci urządzenia (co jest standardową opcją w najnowszych wersjach systemów operacyjnych dla urządzeń mobilnych). Atakujący mając dostęp do naszego emaila, a czasem wręcz zapisanych w plikach numerów kont i haseł, będzie miał bardzo ułatwione zadanie.

Spam, czyli niezamówione wiadomości, to zjawisko mniej niebezpieczne, ale za to znacznie bardziej uciążliwe. Spam może być zarówno legalny (wtedy, gdy pochopnie zgodziliśmy się na otrzymywanie informacji handlowych), jak i nielegalny (gdy wysyłający spam pozyskał kontakt do nas w inny sposób i wykorzystuje go w celach reklamowych bez naszej zgody).

Warto zauważyć, że spam nie zawsze musi być reklamą produktu. Spamem są też np. wysyłane nam przez znajomych „łańcuszki szczęścia" i śmieszne zdjęcia, a także np. prośby o pomoc w ratowaniu bezdomych psów lub zbieraniu nakrętek od butelek. Najważniejszym wyróżnikiem spamu jest to, że wiadomość nie jest kierowana personalnie do nas, tylko do wielu osób, a nasza korzyść z jej otrzymania jest znikoma bądź żadna.

Skutecznymi metodami ochrony przed spamem jest:

- rygorystyczne nieudzialnie zgody na wysyłanie wiadomości handlowych i przetwarzanie danych osobowych (do czego będzie nas namawiać większość przedsiębiorców podpisujących z nami jakiekolwiek umowy, włącznie z operatorami telefonii komórkowej);

- stosowanie filtru antyspamowego w poczcie elektronicznej;

- korzystanie z blokady reklam (np. AdBlock) w wyszukiwarce.

Szczególną uwagę należy zwracać na konkursy promocyjne. Szansa na wygranie odkurzacza jest dla większości osób wystarczającą obietnicą, żeby podały swój adres i zgodę na wysyłanie spamu. Starajmy się unikać takich pokus, bo adres który raz dostał się do spamerskiej bazy danych będzie wykorzystywany stale.

Nie należy także odpowiadać na spam, klikać w linki zamieszczone w podejrzanych wiadomościach ani wyłączać mechanizmów ochrony wbudowanych w klientów poczty, takich jak blokada ładowania zewnętrznych obrazków. Wszelkie takie działania tylko niepotrzebnie przekazują spamerom dodatkowe informacje o adresacie.

POMYSŁ NA LEKCJĘ

Nie trzeba chyba pisać, że internet stanowi jeden z kamieni milowych rozwoju cywilizacji. Wielu z nas nie wyobraża sobie dziś życia bez tego wynalazku. Jednak internet niesie też z sobą pewne zagrożenia, do których należą phishing i spam. Obrona przed nimi może wcale nie być aż tak trudna, dlatego też warto wiedzieć, jak się przed nimi uchronić.

Cele operacyjne

Uczestnicy i uczestniczki:

- wiedzą, czym jest phishing i spam;
- potrafią rozpoznać struktury tekstowe charakterystyczne dla phishingu i spamu;
- rozumieją zagrożenia wiążące się z tymi zjawiskami;
- znają mechanizmy obrony przed niechcianą korespondencją;
- znają zasady bezpiecznego funkcjonowania w sieci.

Przebieg zajęć

1.

Czas: 5 min
Forma: praca indywidualna
Pomoce: załącznik nr 1.

Rozdaj uczniom i uczennicom kartkę ze skopiowanym mailem (**karta pracy**). Poproś, aby przeczytali tekst i zastanowili się, jakie intencje przyświecały nadawcy.

2.

Czas: min
Forma:

Wspólnie z młodzieżą scharakteryzuj język listu i nadawcę. Wnioski zapiszcie na tablicy:

- Na początku pojawia się powitanie.
- Nadawca zwraca się do odbiorcy bardzo poufale, używa formy „ty".
- Nadawca zadaje pytania retoryczne odbiorcy, są one tak sformułowane, by trafiały do odbiorcy (np. każdy chce zrobić prezent osobie, która jest wyjątkowa lub którą kocha).

- Nadawca oferuje pożyczkę, ale nie ujawnia jej szczegółów, czyli odbiorca nie wie, na jaki procent pożyczy pieniądze i ile będzie musiał zwrócić.

- Nadawca używa słów: „najwygodniejsza", „łatwy", „szybki", „wystarczy, że...". Sprawia to wrażenie, że pieniądze są już w zasięgu twojej ręki.

- W zwrocie: „dołącz do nas" – użycie zaimka „nas" zmniejsza dystans między nadawcą a odbiorcą tekstu, masz wrażenie, że z nadawcą już się znacie.

- Użycie trybu rozkazującego – „nie przegap", „skorzystaj" – częsta forma w reklamach.

- Nadawca podaje fałszywą stronę, na którą należy się wejść www.paypai.com. Do złudzenia przypomina ona inną stronę, autentyczną: www.paypal.com. To może sugerować phishing.

Wnioski: Ta wiadomość mailowa jest niewątpliwie spamem i nosi znamiona phishingu. Należy więc nie tylko nie otwierać podanej strony, ale najlepiej ją w ogóle usunąć.

3. Podaj definicje spamu i phishingu.

4. Podziel klasę na 4-5 grup. Poproś, aby każda z nich napisała wiadomość, która będzie zawierała ukryty element phishingu i będzie spamem. Możesz wcześniej przygotować tematy maili, np. zdrowie dziecka, skorzystanie z darmowej porady prawnej, kupno czegoś za okazyjną cenę itp. Następnie poproś, aby grupy zgodnie ze wskazówkami zegara wymieniły się mailami. Każda grupa powinna odnaleźć elementy spamu i phishingu, rozpoznać „haczyki". Podsumuj pracę w grupach.

5. Zapytaj: „Jak bronić się przed spamem i phishingiem?" (burza mózgów). Wnioski zapisz na tablicy (patrz: Wiedza w pigułce).

Ewaluacja

Czy po przeprowadzeniu zajęć ich uczestnicy i uczestniczki:

- rozumieją, że istnieją osoby/instytucje, którym zależy na pozyskaniu poufnych informacji osobistych?

- potrafią zdefiniować phishing i SPAM?

- wiedzą, w jaki sposób bronić się przed SPAM-em i phishingiem?

Opcje dodatkowe

Jeżeli masz czas, możesz poprosić, aby uczniowie i uczennice spisali zasady bezpieczeństwa na dużych, kolorowych kartkach i porozwieszali je na korytarzach szkolnych. W ten sposób podzielą się wiedzą z innymi. Może to stanowić miniprojekt pt.: Bezpieczniej w sieci.

MATERIAŁY

- **Karta pracy**

ZADANIE DLA UCZNIA

Korzystając z dostępnych ci źródeł, napisz definicje słów: pharming i smishing.

SŁOWNICZEK

- **phishing**:

- **spam** : wysyłane automatycznie listy, których wcale nie chcemy dostać. Zwykle zawierają reklamy lub mają cię nakłonić do jakiś działań.

CZYTELNIA

- http://di.com.pl/news/51114,0,Uwaga_na_Doladujeu_Zamiast_doladowania_dostaniesz_aktywacje--Marcin_Maj.html
- `http://www.cert.pl//news/8999/langswitch_lang/pl` (dostęp: 30.12.2014)
- http://www.mbank.pl/aktualnosci/post,5928,mbank-i-zwiazek-bankow-polskich-ostrzegaja-uwaga-na-nowego-wirusa.html (dostęp: 30.12.2014)
- http://di.com.pl/news/50901,0,Dzwonia_z_propozycja_reklamy_w_sieci_Ta_rozmowa_moze_kosztowac_600--700_zl-Marcin_Maj.html (dostęp: 30.12.2014)

Tekst: Radek Czajka, Jarosław Lipszyc, scenariusz: Małgorzata Bazan, konsultacja merytoryczna: Wojciech Budzisz, Łukasz Wojtasik, Michał Woźniak. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/phishing-i-spam/.

Publikacja zrealizowana w ramach projektu Mobilne Bezpieczeństwo, dofinansowanego ze środków Ministerstwa Administracji i Cyfryzacji.

Podstawa programowa:

Informatyka, III poziom edukacyjny
Cele kształcenia
I Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjnokomunikacyjnych.
V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.
Treści nauczania
7. Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania zainteresowań; opisywanie innych zastosowań informatyki; ocena zagrożeń i ograniczeń, aspekty społeczne rozwoju i zastosowań informatyki.

Nowa podstawa programowa:

Informatyka, IV-VIII klasa
Cele kształcenia
Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

Informatyka, liceum i technikum
Treści nauczania
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.