Zasady bezpieczeństwa na portalach społecznościowych.

Podstawowe pojęcia: phishing, kradzież tożsamości.

W dobie Internetu większość z nas ma konto na przynajmniej jednym portalu społecznościowym. Część osób traktuje portale społecznościowe jako źródło informacji o interesujących osobach czy wydarzeniach. Inni przede wszystkim cenią sobie możliwość komunikacji poprzez narzędzia, które dostarcza serwis. Dzięki portalom społecznościowym nie tylko wymieniamy się różnego rodzaju informacjami, ale także publikujemy osobiste zdjęcia, materiały video, reklamujemy się. Choć portale społecznościowe wydają się stosunkowo bezpieczne, to niestety można spotkać tam sporo zagrożeń, które mogą nieść ze sobą przykre konsekwencje nie tylko dla nas, ale także naszych znajomych. Jednym z zagrożeń jest phishing.

Phishing *– metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.*

Zjawiskiem powiązanym z phishingiem jest kradzież tożsamości. Po co oszustom czyjaś tożsamość? Np. mogą założyć fałszywe konto na eBay i handlować w czyimś imieniu. Oszukani ludzie znają wtedy tylko ukradzioną przez oszusta tożsamość, która należy do zupełnie niewinnej osoby. Ukradziona tożsamość może przydać się jeszcze do wielu innych oszustw, niekoniecznie internetowych, ale łączących się z podrobionymi dokumentami.

Na portalu społecznościowym cyberprzestępcy mogą:

- rozsyłać linki do fałszywych stron logowania w celu wyłudzenia haseł i innych danych osobowych
- rozsyłać reklamy i spam, które zaciekawiają, a niosą groźną zawartość. Użytkownik, klikając w zamieszczony na portalu link np. loguje się na fałszywą stronę i podaje dane, których podać nie powinien. Te reklamy często wykorzystują ciekawość użytkowników i ich łatwowierność oferując nieistniejące funkcje lub usługi (np: Sprawdź kto ogląda Twój profil na Facebooku? Poznaj sposób na zarabianie 6000 euro dziennie bez wychodzenia z domu, To cudowne lekarstwo Ci pomoże…itp.)
- zamieszczać w serwisach społecznościowych odnośniki do aplikacji (lub bezpośrednio aplikacje) żądające dostępu do konta w serwisie społecznościowym, aby następnie pobrać z niego część danych lub zainstalować niechciane programy.

Zdarza się, że użytkownicy portali społecznościowych sami, w sposób zupełnie niefrasobliwy bądź przez nieuwagę zamieszczają zdjęcia, filmy, zawierające w treści dane wrażliwe, których nie powinno się ujawniać, np. zdjęcia dokumentów.

Po uzyskaniu nieuprawnionego dostępu do czyjegoś konta na portalu społecznościowym cyberprzestępcy mogą:

1. Sprzedać te dane na czarnym rynku w celu wykorzystania ich w celach przestępczych,
2. Z biegiem czasu zebrać większą ilość informacji z ukradzionego konta,
3. Wysyłać spam z zaatakowanego konta do innych użytkowników portalu,
4. Wysyłać wiadomości do znajomych ofiary włamania (np. z prośbą o przelanie pieniędzy w „nagłej potrzebie” itp.),
5. Rozsyłać znajomym właściciela konta linki do stron phishingowych (wyłudzających dane wrażliwe) lub zawierających szkodliwe oprogramowanie.

Facebook zgadza się, by niezależni programiści mogli dodawać przygotowywane przez siebie aplikacje. Często tego typu programy proszą użytkowników o dostęp do informacji osobistych, a przy okazji mogą łatwo sprawić, że ujawnione zostaną także inne dane, które interesują przestępców. Choć serwisy takie jak Facebook zdają sobie sprawę z istnienia tego procederu, to jednak sprawdzenie kilkudziesięciu tysięcy aplikacji, gdy wciąż napływają nowe, jest fizycznie niemożliwe. W takim przypadku zawiedzie nawet ochrona antywirusowa, gdyż szkodliwe oprogramowanie jest uruchamiane z poziomu serwera portalu społecznościowego. Pozostaje zatem liczyć na czujność pracujących tam analityków oraz samych użytkowników portalu.

W ostatnich latach niektórzy naukowcy zaczęli ostrzegać przed możliwością uzależnienia od serwisów społecznościowych. Problem ten dotyczy przede wszystkim młodych ludzi, którzy spędzają np. na Facebooku kilka godzin dziennie. Według naukowców nie mogą oni poradzić sobie z rosnącym zaangażowaniem w to, co dzieje się aktualnie na Facebooku. Presja zalogowania się i sprawdzenia informacji dotyczących znajomych, obejrzenia ich najnowszych zdjęć oraz porównania wyników gier, jest tak silna, że zapominają o innych aspektach życia. Bywa to przyczyną gorszych wyników w nauce, a potem w pracy.

Pod adresem Facebooka wysuwane są zarzuty rejestrowana życia użytkowników tego serwisu, a także osób powiązanych z tymi użytkownikami np. ich rodziny, przyjaciół, którzy niekoniecznie są użytkownikami portalu, ale przewijają się na zdjęciach, filmach itp. Facebook jest też przez niektórych posądzany o monitorowanie użytkowników i wdrażanie nowych funkcji bez pytania ich o zgodę

(nowe funkcje są domyślnie włączone). W 2012 zdarzyło się, że Facebook zorganizował na próbie 700 tysięcy użytkowników bez ich zgody eksperyment psychologiczny, mający na celu stwierdzić, czy da się manipulować uczuciami osób przez Internet. Informacja o tym eksperymencie wyszła na jaw dopiero dwa lata później.

Podstawowe zasady bezpieczeństwa na portalach społecznościowych.

Aby uniknąć oszustw należy przede wszystkim:

- Stosować silne hasła,
- Używać programy antywirusowe i antyszpiegowskie,
- Posiadać świadomość możliwych do pojawienia się zagrożeń, związanych z portalami społecznościowymi – np. podszywania się innych osób pod czyjąś tożsamość. Aby stwierdzić takie oszustwo wystarczy czasami np. telefon do znajomego.
- Unikać podawania wrażliwych danych osobowych, które mogłyby być wykorzystane przez przestępców (nr pesel, nr konta bankowego, haseł do kont)
- Unikać zamieszczania zdjęć dokumentów oraz zdjęć osobistych, które mogłyby być wykorzystane przez przestępców.
- Unikać zamieszczania krytycznych opinii nt. innych osób, które mogłyby być powodem procesów o zniesławienie,

Spam i phishing często pojawiają się równolegle: oszuści masowo wysyłają wiadomości e-mail z nadzieją, że uda im się wyłudzić od odbiorców określone informacje. Dla nich należące do użytkowników dane osobowe mają bardzo dużą wartość, a więc często są one na celowniku, co potwierdzają publikowane w mediach historie. Ogólnie celem takich wiadomości jest uzyskanie dostępu do kont użytkowników lub numerów kart płatniczych za pośrednictwem rozsyłanego pocztą phishingu czy socjotechniki.

Zadanie 1: Sprawdź czy wybrany portal społecznościowy posiada łącze szyfrowane z certyfikatem bezpieczeństwa.
Zadanie 2: Przejrzyj stronę www.oszustwsieci.pl

Źródło:
Wikipedia
www.oszustwsieci.pl

Zajęcia zrealizowane w ramach projektu **„Trzecia Misja Uczelni - szansą dla rozwoju pasji, zainteresowań i edukacji dla osób zagrożonych wykluczeniem społecznym”** w ramach Programu Operacyjnego Wiedza Edukacja Rozwój współfinansowanego ze środków Europejskiego Funduszu Społecznego