

Co roku tysiące użytkowników pada ofiarą oszustw internetowych. Umiejętność rozpoznania zagrożenia jest najlepszą ochroną, dlatego laboratorium PandaLabs przedstawiło listę najpowszechniejszych pułapek zastawianych na internatów. Skutkiem takich oszustw może być nawet znaczna utrata środków finansowych. Nie dajmy się nabrać!

PandaLabs, laboratorium antywirusowe firmy Panda Security, przygotowało ranking najpopularniejszych oszustw z ostatnich kilku lat. Wszystkie te sztuczki wykorzystujące zaufanie ofiary mają ten sam cel: wyłudzenie od użytkowników pieniędzy. Ukradzione kwoty wynoszą od 500 do 1000 dolarów.

Takie oszustwa wpisują się zwykle w podobny schemat: pierwszym krokiem jest nawiązanie kontaktu przez e-mail lub sieci społecznościowe, w którym ofiara proszona jest o odpowiedź za pomocą poczty elektronicznej, telefonu czy faksu. Gdy użytkownik chwyci przynętę, przestępcy będą starali się zdobyć jego zaufanie, prosząc w końcu o jakąś sumę pieniędzy pod tym czy innym pretekstem.

Luis Corrons, dyrektor techniczny laboratorium PandaLabs stwierdził: „Podobnie jak w przypadku klasycznych oszustw sprzed ery internetu, wielu użytkowników, którzy stają się ofiarami oszustwa on-line i tracą pieniądze, nie zgłasza przestępstwa. Już dawniej odzyskanie straconych pieniędzy było trudne, a teraz jest to jeszcze trudniejsze, gdyż ślady przestępców giną w sieci. Najlepszą ochroną jest wiedza o tym, jak rozpoznawać takie oszustwa i nie dać się nabrać”.

PandaLabs opracowało ranking najpopularniejszych oszustw ostatnich dziesięciu lat na podstawie sposobu ich dystrybucji i częstotliwości występowania:

1.Oszustwo nigeryjskie: To pierwszy typ oszustwa, jaki pojawił się w internecie, często stosowany przez cyberprzestępców, aż do dzisiaj. Najczęściej ma formę e-maila, rzekomo od osoby, która musi odzyskać dużą sumę pieniędzy od jakiegoś kraju (zwykle jest to Nigeria, stąd nazwa). Za pomoc obiecuje wysoką nagrodę. Użytkownicy, którzy w to uwierzą, są proszeni o przelanie pewnej sumy na pokrycie opłat bankowych (często około 1000 dolarów). Po zapłaceniu kwoty kontakt zanika, a pieniądze przepadają.

2.Loterie: Podobne do oszustwa nigeryjskiego. Użytkownik otrzymuje e-mail z informacją, o rzekomej wygranej w loterii i prośbą o dane osobowe w celu przekazania zwycięzcy wysokiej nagrody. Tak jak w przypadku poprzedniego oszustwa - ofiary proszone są o zaliczkę w wysokości około 1000 dolarów na pokrycie opłat bankowych itp.

3.Dziewczyny: Piękna dziewczyna, zwykle Rosjanka, znajduje adres e-mail użytkownika, którego chce poznać. Jest młoda i marzy o przyjeździe do kraju ofiary i spotkaniu, ponieważ jest po uszy zakochana. Chce przyjechać natychmiast, lecz w ostatniej chwili pojawia się problem i okazuje się, że nie posiada wystarczających środków finansowych na podróż. Prosi, więc o gotówkę (i w tym przypadku jest to około 1000 dolarów) na opłacenie biletów lotniczych, wizy itp. Łatwo zgadnąć, że pieniądze i dziewczyna przepadają.

4.Oferty pracy: Tym razem użytkownik otrzymuje wiadomość od zagranicznej firmy poszukującej agentów finansowych w jego kraju. Praca jest łatwa – można ją wykonywać w domu – i pozwala zarobić do 3000 dolarów przy 3-4 godzinach pracy dziennie. Jeśli ofiara się zgodzi, zostaje poproszona o dane bankowe. Użytkownik jest wykorzystywany do kradzieży pieniędzy z kont bankowych osób, których dane zostały wcześniej skradzione przez cyberprzestępców. Pieniądze są przelewane bezpośrednio na konto ofiary, która jest proszona o przesłanie sumy przez Western Union. Ofiara staje się tzw. „słupem”, a w policyjnym śledztwie w sprawie kradzieży uznawana jest za współsprawcę. Mimo, że praktyka ta jest często określana jako scam, czyli wyłudzenie, różni się od innych oszustw tego typu tym, że „słup” również może czerpać korzyści, choć nieświadomie popełnia przestępstwo.

5.Facebook / Hotmail: Przestępcy uzyskują dane dostępowe do Facebooka, poczty Hotmail lub podobnych serwisów. Następnie mogą zmienić dane do logowania, tak by prawdziwy użytkownik nie mógł korzystać z konta. Oszuści wysyłają do wszystkich kontaktów wiadomość o tym, że użytkownik wyjechał na wakacje (często do Londynu) i

został obrabowany tuż przed powrotem do domu. Wciąż posiada on bilety lotnicze, ale potrzebuje około 500-1000 dolarów na hotel.

6.Odszkodowanie: Stosunkowo nowy rodzaj wyłudzenia, bazujący na oszustwie nigeryjskim. Użytkownik otrzymuje e-mail informujący o rzekomym utworzeniu funduszu wypłacającego odszkodowania ofiarom oszustwa nigeryjskiego. Ofiara może otrzymać odszkodowanie (często około 1 miliona dolarów), ale tak jak w przypadku pierwotnego oszustwa, musi oczywiście wpłacić zaliczkę w wysokości około 1000 dolarów.

7.Pomyłka: Bardzo popularny rodzaj oszustwa w ostatnich miesiącach, być może związany w kryzysem finansowym i trudnościami w sprzedaży towarów i domów. Oszuści kontaktują się z osobą, która zamieściła ogłoszenie o sprzedaży domu, samochodu itp. Z wielkim entuzjazmem zgadzają się kupić oferowany towar i wkrótce przysyłają czek, ale na niewłaściwą sumę (zawsze wyższą od uzgodnionej). Sprzedawca jest proszony o zwrócenie różnicy. Czeku nie można zrealizować, dom pozostaje niesprzedany, a ofiara traci przelane pieniądze.

Co zrobić, jeśli stanę się celem jednego z tych oszustw?

To normalne, że jeśli nie wiesz nic o przestępczych sztuczkach tego rodzaju, możesz sądzić, że wygrałeś w loterii lub znalazłeś miłość w internecie. Oto kilka praktycznych rad, które pomogą ci uniknąć kłopotów:

Zainstaluj dobry program antywirusowy, który potrafi wykrywać spam.

Kieruj się zdrowym rozsądkiem. To twój najlepszy sojusznik w obronie przed wyłudzeniami. Nikt nie rozdaje niczego za darmo, a miłość od pierwszego wejrzenia w internecie zdarza się bardzo rzadko.

Internet jest fantastycznym narzędziem o wielu zastosowaniach, ale jeśli naprawdę chcesz coś sprzedać, lepiej zobaczyć sprzedawcę na własne oczy. Nawet jeśli nawiążesz kontakt przez sieć, lepiej dokonać transakcji w „prawdziwym świecie”, aby upewnić się, że ewentualni nabywcy mają szczerą intencję.

Jeśli jednak padniesz ofiarą oszustwa PandaLabs zaleca niezwłocznie zgłosić przestępstwo policji. „Mimo że ściganie takich przestępstw może być skomplikowane, organy ścigania coraz lepiej radzą sobie z cyberprzestępcami” - mówi Corrons.

Więcej informacji na stronie www.pandalabs.com

Panda Security Polska