Dzisiaj Dzień Bezpiecznego Komputera- ekspert radzi, jak być bezpiecznym w sieci nie tylko od święta

**Dzisiaj obchodzimy Dzień Bezpiecznego Komputera, jednak o bezpieczeństwo powinniśmy dbać zawsze, a nie tylko od święta. Codziennie czytamy informację o nowych atakach phishingowych skierowanych do określonej grupy odbiorców, niestety w wielu przypadkach skutecznych. Ofiary ponoszą różnego rodzaju straty, o czym dowiesz się z poniższego tekstu.**

Czym jest phishing?

To słowo z języka angielskiego, niemające jeszcze utrwalonego odpowiednika w języku polskim. Phishing to oszustwo internetowe polegające na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia wrażliwych danych (danych osobowych, kontaktowych, logowania, haseł, numerów kart bankowych wraz z kodami CVV i innych istotnych informacji) lub zainfekowania komputera albo telefonu komórkowego złośliwym oprogramowaniem.

**Dane te są wykorzystywane do różnych działań przestępczych, przykładowo:**

1. kradzieży środków z rachunków w instytucjach finansowych,
2. kradzieży tożsamości celem zaciągnięcia pożyczek lub kredytów,
3. przejęcia naszych kont w serwisach społecznościowych czy platformach zakupowych,
4. wynajmu mieszkania, hotelu czy samochodu,
5. kupna różnego rodzaju dóbr w naszym imieniu,
6. zakładania rachunków bankowych i kont w innych instytucjach finansowych, które następnie wykorzystywane są w procesie prania pieniędzy,
7. sprzedaży naszych danych w celu dalszego rozpowszechniania spamu lub phishingu bądź popełniania innego rodzaju przestępstw.

Zjawisko to jest groźne z wielu względów, a przestępcy niestety są coraz lepiej przygotowani do skutecznej kradzieży. Najczęściej docierają do nas za pomocą e-maila lub SMS-a.

Jak rozpoznać phishing?

Trzeba zwrócić uwagę na kilka przykładowych elementów:

1. Strony internetowe, na które jesteśmy przekierowywani w wyniku kliknięcia w fałszywy link łudząco przypominają prawdziwą stronę, np. banku. Jeszcze niedawno w radach dotyczących tego, jak wykryć fałszywą witrynę, wskazywano m.in. na słabej jakości grafikę lub błędy językowe. Dzisiaj to już rzadkość. Przestępcy idealnie odwzorowują oryginalną stronę, dbają o jej poprawność językową, szczegóły, tak aby jak najwierniej naśladowała pierwowzór.
2. Innym elementem, wobec którego wskazuje się na konieczność jego sprawdzenia, jest adres strony internetowej, na której przebywamy. Czasami adres fałszywej strony jest zupełnie inny od prawdziwej i wtedy mamy pewność, że znaleźliśmy się tam, gdzie być nie powinniśmy. Jednak najczęściej przestępcy wymyślają adres łudząco podobny do adresu strony oryginalnej, różniący się tylko jakimś drobnym elementem (zamienione kolejnością znaki, wstawiony w adresie myślnik lub akcent przy literze, np. ogonek, dwie kropki itd.). Najbardziej podstępnym sposobem jest wstawienie do adresu litery z innego alfabetu wyglądającej identycznie lub bardzo podobnie (niestety są takie litery) - wykrycie tego zabiegu jest bardzo trudne, nawet dla specjalisty.
3. Zbieżność czasowa otrzymania wiadomości z realną sytuacją w naszym życiu. Dobrym przykładem jest oczekiwanie na przesyłkę i otrzymanie wiadomości SMS o konieczności dopłaty za paczkę z powodu jej większego ciężaru lub zmiany cennika albo niemożności wysłania z centrum dystrybucyjnego. Ileż takich akcji phishingowych przeprowadzono w okresie pandemii, kiedy większość z nas kupowała online i czekała na dostarczenie towaru. Inny przykład może stanowić sytuacja, w której czynny użytkownik Facebooka otrzymuje wiadomość o nietypowej aktywności zarejestrowanej na jego koncie z prośbą o podanie hasła, rzekomo w celu zabezpieczenia profilu. Kreatywność przestępców jest tu nieograniczona i zwykle dostosowana do aktualnej rzeczywistości, tak aby otrzymana wiadomość nie budziła podejrzeń, miała nasz osobisty kontekst.
4. Manipulacja polegająca na grożeniu, zastraszaniu, wzbudzaniu naszego niepokoju. Wiadomość o niedopłacie za gaz w sezonie grzewczym i grożenie jego odcięciem, wiadomość o niedopłacie podatku, mandacie, wykryciu niedozwolonych treści na komputerze itd. Mimo że te schematy są znane i wielokrotnie opisane, kiedy emocje biorą górę, czujność każdego może być narażona na szwank.

**Aktualnie pojawiają się nowe odmiany phishingu, w tym:**

1. **Voice phishing (vishing)**, czyli oszustwo głosowe (np. podszycie się pod pracownika banku) dokonywane za pomocą techniki tzw. spoofingu, która polega na sfałszowaniu identyfikatora dzwoniącego (na ekranie telefonu będziemy widzieć, że dzwoni bank),
2. **Deepfake phishing**, a więc użycie obrazu osoby (realnej lub nieistniejącej) wygenerowanego przez sztuczną inteligencję w celu uwiarygodnienia kontaktu/oferty.

Jakie zagrożenia niesie przyszłość?

Z pewnością przestępcy będą coraz szerzej korzystać ze sztucznej inteligencji. Już dzisiaj odnotowywane są próby podszywania się przy pomocy wygenerowanego przez sztuczną inteligencję głosu w popularnej ciągle metodzie wyłudzeń „na wnuczka”. Osoby starsze, mogące mieć osłabiony słuch, są tu szczególnie narażone. Pojawiły się również fałszywe reklamy, w których znane osoby - a właściwie ich wizerunki wygenerowane przez sztuczną inteligencję - zachęcają do intratnych inwestycji. W miarę postępu technologii coraz trudniej będzie odróżnić to, co prawdziwe, od tego, co fałszywe.

**I dlatego:**

1. Zawsze stosujemy zasadę ograniczonego zaufania - wszystko może być oszustwem.
2. Zwracamy uwagę nietypowe prośby od członka rodziny, współpracownika czy używanego przez nas serwisu, zwłaszcza jeśli dotyczą przekazania poufnych danych, przelania środków pieniężnych, instalacji oprogramowania itp.
3. Przyjrzyjmy się dokładniej szczegółom: adresowi strony, danych nadawcy e-maila czy dzwoniącej do nas osoby, grafikom, językowi, zwłaszcza w kontekście składni i błędów.
4. Jeśli po przeczytaniu wiadomości odczujemy silną emocję zaciekawienia czy strachu albo pilną potrzebę działania, to jest to sygnał ostrzegawczy, że możemy być manipulowani.
5. Pośpiech naszych czasów niestety sprzyja przestępcom. Liczą na to, że zadziałamy szybko, bez zastanowienia, automatycznie, w przerwie pomiędzy innymi ważnymi rzeczami.
6. Chcąc potwierdzić wiadomość z nadawcą nigdy nie używajmy danych kontaktowych podanych w wiadomości lub na stronie, do której otrzymaliśmy link. Musimy je znaleźć w niezależnym źródle.
7. Do każdego serwisu używamy innego/unikalnego hasła. Użycie menedżera haseł ułatwia ten proces.
8. Tam, gdzie to możliwe, włączamy podwójne uwierzytelnienie i nigdy nie podajemy jednorazowych kodów osobom trzecim ani w żaden inny sposób nie autoryzujemy działań, których sami nie podejmujemy.

**Dariusz Polaczyk** - Risk&Security Manager w Currency One SA