fundacja instytut
CYBERBEZPIECZEŃSTWA

Seniorzy a cyberbezpieczeństwo

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Rozwój internetu i nowych technologii w ostatnich latach dostarczył dużo nowych rozwiązań i usług, które stały się integralną częścią życia wielu osób. Wraz z rozwojem technologicznym pojawiły się jednak także zagrożenia związane z cyberbezpieczeństwem. Grupą szczególnie podatną na takie zagrożenia są osoby starsze, które padają ofiarami przestępstw internetowych. Cyberprzestępcy, wykorzystując brak znajomości technologii u tych osób, narażają je na utratę pieniędzy.

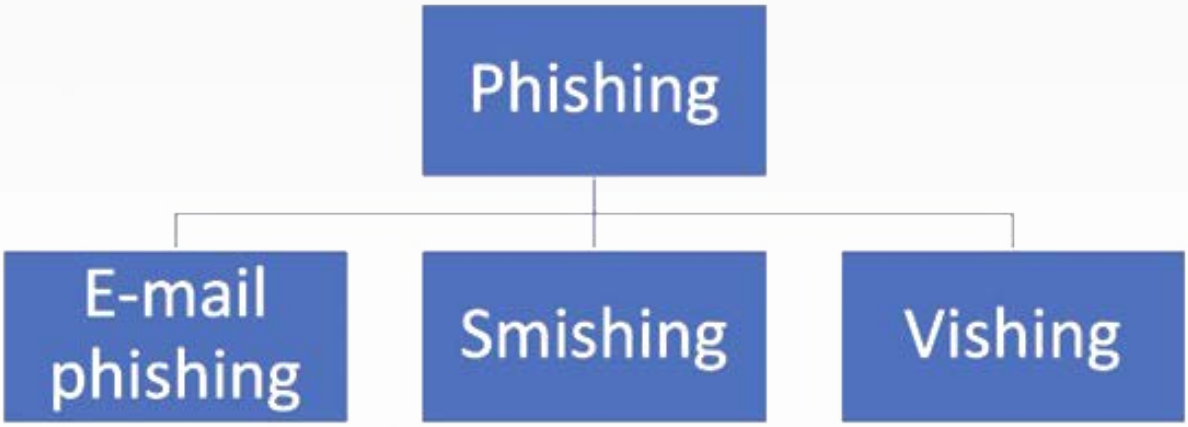
Seniorzy w sieci

Badanie InfoSenior 2023 przeprowadzone na zlecenie Warszawskiego Instytutu Bankowości (WIB) we współpracy ze Związkiem Banków Polskich (ZBP) zwraca uwagę na wzrost aktywności internetowej osób starszych[1]. Zgodnie w przedstawionymi wynikami 82 proc. badanych seniorów posiada konto internetowe w banku, a 75 proc. opłaca większość swoich zakupów kartami płatniczymi. Za zakupy w internecie zaś co trzeci ankietowany płaci online. Spośród badanych seniorów 62 proc. wskazało, że miało styczność bezpośrednio lub w swoim otoczeniu z próbami wyłudzenia pieniędzy w przestrzeni cyfrowej, a 55 proc. z nich ocenia przeciętnie swój poziom wiedzy w zakresie bezpiecznego korzystania z internetu, w tym bankowości internetowej. W porównaniu do badania z 2019 r. do 10 proc. wzrósł odsetek seniorów, którzy podczas korzystania z internetu w większym stopniu polegają na intuicji niż na zasadach bezpieczeństwa i oceniają swój poziom wiedzy jako słaby. Badanie ponadto pokazuje, że ponad połowa seniorów pomaga finansowo swoim dzieciom lub wnukom. Przedstawione dane uzmysławiają, że istnieje potrzeba zwiększania świadomości seniorów na temat cyberbepieczeństwa i uodporniania ich na zagrożenia w sieci.

1 *ZBP/WIB: co trzeci polski senior kupuje i płaci online*, Związek Banków Polskich, 21.01.2023 r., https://zbp.pl/Aktualnosci/Wydarzenia/Infosenior2023 [dostęp: 24.05.2023].

Cyberzagrożenia

Jednym z największych zagrożeń dla seniorów w sieci jest *phishing*. Technika ta wykorzystuje inżynierię społeczną, a przestępcy, podszywając się pod wybrane podmioty, próbują oszukać osobę poprzez nakłonienie jej do określonych działań. Celem phishingu jest wyłudzenie istotnych danych np. do logowania do kont bankowych czy mediów społecznościowych. Istnieją różne rodzaje phishingu, ale w kontekście zagrożeń dla seniorów najważniejsze są te, które przedstawia poniższa grafika.



W przypadku e-mail phishingu oszuści wysyłają maile, podszywając się pod określoną instytucję w celu skłonienia ofiary do ujawnienia poufnych informacji. Wiadomości wysyłane przez cyberprzestępców często zawierają także linki do stron internetowych rozprzestrzeniających szkodliwe oprogramowanie. Ponadto do e-maili mogą być też dołączane pliki PDF, których otwarcie może wyrządzić szkody na urządzeniach ofiar[2]. Drugi rodzaj phishingu to *smishing*, polegający na podszywaniu się w wiadomości SMS. Również w tym przypadku oszuści starają się nakłonić osobę do określonych działań, takich jak otworzenie zainfekowanych stron internetowych, wykonanie przelewu lub podanie danych[3]. Coraz częściej do oszustw wykorzystuje się także portale

2 M. Frączak, *Phishing ma różne oblicza. Uwaga na złośliwe załączniki PDF*, Polityka Bezpieczeństwa, 26.05.2022 r., https://www.politykabezpieczenstwa.pl/pl/a/phishing-ma-rozne-oblicza-uwaga-na-zlosliwe-zalaczniki-pdf [dostęp: 24.05.2023].

3 M. Mazur, *Phishing, smishing, vishing – jak się w tym połapać?*, Bulldogjob, 27.01.2021 r., https://bulldogjob.pl/readme/phishing-smishing-vishing-jak-sie-w-tym-polapac [dostęp: 24.05.2023].

społecznościowe, na których wysyłana jest atrakcyjna oferta zawierająca link do zainfekowanej strony.

Inna odmianą phishingu jest *vishing*, czyli metoda oszustwa polegająca na przeprowadzeniu rozmowie telefonicznej z ofiarą i wyłudzeniu od niej danych. Oszuści dzwoniący do niej podszywają się pod określoną osobę i próbują wyłudzić wrażliwe dane albo skłonić ofiarę do przekazania im dostępu do komputera za pośrednictwem tzw. zdalnego pulpitu. Popularnym oszustwem z wykorzystaniem vishingu jest tzw. metoda na wnuczka. Przestępcy podszywają się w niej pod kogoś

spokrewnionego z ofiarą i proszą o szybkie wsparcie finansowe. Wśród innych sposobów na wprowadzenie w błąd popularne jest też podszywanie się pod pracownika banku, sanepidu czy też doradcę inwestycyjnego. Na oszustwa tego typu są narażone w szczególności osoby starsze[4]. Mimo że w ostatnich latach wzrosła świadomość zagrożeń z wykorzystaniem vishingu, to rozwój nowych technologii daje bardziej zaawansowane możliwości podszywania się. Sztuczna inteligencja umożliwia obecnie generowanie zdań wypowiadanych głosem danej osoby, jeżeli dysponuje się kilkusekundową próbką tego głosu. Dalszy rozwój i upowszechnienie tej technologii może sprawić, że oszuści będą mogli zadzwonić do wybranej osoby, podszywając się pod jej bliskich. Jeśli głos wygenerowany za pomocą sztucznej inteligencji nie wzbudzi podejrzeń, w łatwy sposób będą mogli np. przekonać kogoś do podania wrażliwych danych osobowych, danych do logowania czy też do zrobienia przelewu. Do wykradzenia informacji może być także wykorzystywany callerID spoofing, który umożliwia, za pomocą ogólnodostępnych narzędzi w sieci, podszywanie się pod dowolny numer telefonu[5].

Phishing nie jest jednak jedynym zagrożeniem dla seniorów w sieci. Coraz częściej wykorzystywaną formą oszustwa staje się także *wangiri fraud*, w którym przestępcy wykorzystują połączenia telefoniczne w celu wyłudzenia pieniędzy. Posługują się oni zagranicznymi numerami telefonów, wyglądającymi na pierwszy rzut oka na polskie, i wykonują krótkie, trwające jeden sygnał połączenia na wybrane numery użytkowników, tak aby dana osoba nie zdążyła odebrać. Następnie, podczas oddzwaniania, kiedy dzwoniący słyszy sygnał oczekiwania

4 W. Krawczyk, *Phishing, smishing, vishing… Jak nie dać się oszukać*, Obserwator Finansowy, 18.05.2023 r., https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/oszustwa-bezgotowkowe/?gclid=CjwKCAjw67ajBhAVEiwA2g_jEFHnTevAfM1Jtxn_MVY9nLBxnqP79Cx1gqJS_Dbpw8V6vqNbm6XfhoCefcQAvD_BwE [dostęp: 24.05.2023].

5 A. Rudra, *What Is Caller ID Spoofing?*, PowerDMARC, 25.08.2022 r., https://powerdmarc.com/what-is-caller-idspoofing/ [dostęp: 24.05.2023].

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

albo zajętego numeru, naliczane są koszty za połączenie[6]. Samo określenie *wangiri* pochodzi z japońskiego słowa *wankiri*, które można przetłumaczyć jako „jedno cięcie". Odnosi się to do sposobu działania przestępców, czyli wysłania jednego sygnału, ucięcia połączenia i liczenia na to, że dana osoba oddzwoni. Aby do tego skłonić, oszuści stosują numery zagraniczne, których prefiksy są podobne do polskich połączeń międzymiastowych, co zwiększa szanse na to, że osoba się pomyli. Przykładowo numer kierunkowy Warszawy to +22, a Wybrzeża Kości Słoniowej +225. Formą oszustwa popularną obecnie w USA, której ofiarą padają seniorzy, jest również *tech support fraud*. Polega ona na tym, że cyberprzestępcy

podają się za inżynierów wsparcia technicznego, rzekomo usuwających usterkę z komputera albo rachunku bankowego ofiary. W rzeczywistości dokonują kradzieży środków pieniężnych[7].

Osoby starsze często zmagają się także z samotnością i szukają znajomości na portalach randkowych lub w mediach społecznościowych. Jest to wykorzystywane przez oszustów, którzy nawiązują z nimi kontakt, budują relacje, okazują zainteresowanie ich życiem oraz problemami, a następnie wyłudzają pieniądze. Ofiarami takich przestępstw nierzadko padają samotne kobiety, oszukane przez poznanego w sieci mężczyznę. Na początku tworzy on z nimi więź, wzbudza zaufanie, obiecuje spotkanie, po czym informuje ofiarę, że popadł w poważne problemy finansowe i potrzebuje pomocy.

Zmanipulowana osoba, która chce pomóc, przelewa swoje oszczędności albo nawet bierze kredyt w celu udzielenia pomocy poznanej osobie. Oszust natomiast zrywa kontakt, a utraconych pieniędzy często nie da się odzyskać.

6 M. Zagańczyk, *T-Mobile: seniorze, uważaj na te numery! To może być wangiri fraud!*, Telepolis, 5.05.2020 r., https://www.telepolis.pl/wiadomosci/bezpieczenstwo/t-mobile-seniorze-uwazaj-na-te-numery [dostęp: 24.05.2023].

7 P. Muncaster, *Tech support scammers are still at it: Here's what to look out for in 2023*, WeLiveSecurity, 19.01.2023 r., https://www.welivesecurity.com/2023/01/19/tech-support-scammers-still-at-it-what-look-out-for/ [dostęp: 24.05.2023].

Podsumowanie

Seniorzy stanowią jedną z bardziej narażonych grup na niebezpieczeństwa w sieci. Pomimo upowszechniania wiedzy na temat cyberzagrożeń padają oni ofiarami oszustów. Rozwój technologiczny sprawia, że pojawiają się coraz bardziej wyrafinowane metody przestępstw internetowych, przez co konieczne jest podejmowanie działań zwiększających umiejętności cyfrowe wśród osób starszych oraz podnoszących ich świadomość na temat zagrożeń w sieci. Ważna rolę odgrywają przedsięwzięcia edukacyjne, a także kampanie informacyjne prowadzone przez instytucje państwowe i przedsiębiorstwa.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

Bibliografia

Frączak M., *Phishing ma różne oblicza. Uwaga na złośliwe załączniki PDF*, Polityka Bezpieczeństwa, 26.05.2022 r., https://www.politykabezpieczenstwa.pl/pl/a/phishing-ma-rozneoblicza-uwaga-na-zlosliwe-zalaczniki-pdf [dostęp: 24.05.2023].

Krawczyk W., *Phishing, smishing, vishing… Jak nie dać się oszukać*, Obserwator Finansowy, 18.05.2023 r., https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/oszustwabezgotowkowe/?gclid=CjwKCAjw67ajBhAVEiwA2g_jEFHnTevAfM1Jtxn_MVY9nLBxnqP7 9Cx1gqJS_Dbpw8V-6vqNbm6XfhoCefcQAvD_BwE [dostęp: 24.05.2023].

Mazur M., *Phishing, smishing, vishing – jak się w tym połapać?*, Bulldogjob, 27.01.2021 r., https://bulldogjob.pl/readme/phishing-smishing-vishing-jak-sie-w-tym-polapac [dostęp: 24.05.2023].

Muncaster P., *Tech support scammers are still at it: Here's what to look out for in 2023*, 19.01.2023 r., https://www.welivesecurity.com/2023/01/19/tech-support-scammers-still-at-itwhat-look-out-for/ [dostęp: 24.05.2023].

Rudra A., *What Is Caller ID Spoofing?*, PowerDMARC, 25.08.2022 r., https://powerdmarc.com/what-is-caller-id-spoofing/ [dostęp: 24.05.2023].

Zagańczyk M., *T-Mobile: seniorze, uważaj na te numery! To może być wangiri fraud!*, Telepolis, 5.05.2020 r., https://www.telepolis.pl/wiadomosci/bezpieczenstwo/t-mobile-seniorze-uwazajna-te-numery [dostęp: 24.05.2023].

ZBP/WIB: co trzeci polski senior kupuje i płaci online, Związek Banków Polskich, 21.01.2023 r., https://zbp.pl/Aktualnosci/Wydarzenia/Infosenior2023 [dostęp: 24.05.2023].

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości