Załącznik nr 3 do SOPZ

Informacje o zagrożeniach w sieci związanych z fałszywymi stronami internetowymi oraz sposobach unikania ich

FAŁSZYWE STRONY w internecie. Jak je rozpoznać?

JEDNYM z wielu rodzajów zagrożeń w Internecie są FAŁSZYWE STRONY, do których często prowadzą linki, odsyłacze czy przekierowania na strony podszywające się pod znane strony lub serwisy, z których korzystamy na co dzień. Na linki prowadzące do fałszywych stron można się natknąć nie tylko w internecie, ale również w emailach czy SMS-ach.

KAŻDY z nas może natknąć się na taką stronę!

Przykłady z życia:

1. Mieszkanka powiatu kędzierzyńsko-kozielskiego otrzymała sms-a z informacją o zaległości za usługę telefoniczną w wysokości 1,47 zł. W wiadomości znajdował się również link do strony internetowej banku. Po kliknięciu na niego, kobieta została przekierowana na fałszywą stronę, przez co straciła z konta 18 tys. zł.
2. Ponad 3 tys. zł straciła mieszkanka Chełma odpowiadając na identycznego sms-a. Gdy dokonała wpłaty na wskazane konto okazało się, że z jej rachunku pobrana została dużo większa kwota.
3. Policja zaleca, aby wystrzegać się sytuacji jak taka, gdy oszuści, którzy pod pretekstem zakupu towaru wystawionego za pośrednictwem jednej z popularnych platform zakupowych , przesyłają link przekierowujący do łudząco podobnej witryny tej platformy z instrukcją do wprowadzenia karty płatniczej, w celu rzekomego szybkiego przelania pieniędzy. W ten sposób przestępcy uzyskują dostęp do środków finansowych sprzedającego.

Dodatkowe źródła informacji:

Uwaga na fałszywe sms-y zawierające linki do dokonania płatności - Aktualności - Policja.pl
https://policja.pl/pol/aktualnosci/170506,Uwaga-na-falszywe-sms-y-zawierajace-linki-do-dokonania-platnosci.html

Uważajcie na oszustwa internetowe! - Aktualności - Policja.pl
https://www.policja.pl/pol/aktualnosci/196581,Uwazajcie-na-oszustwa-internetowe.html

SMS-owe oszustwa. Dostałeś taką wiadomość? Uważaj (komputerswiat.pl)
https://www.komputerswiat.pl/aktualnosci/wydarzenia/sms-owe-oszustwa-dostales-taka-wiadomosc-uwazaj/y3xef7q

Uwaga! Oszuści wysyłają fałszywe linki wykorzystując portal OLX oraz aplikację Whatsapp - Wiadomości - Komenda Miejska Policji w Bielsku-Białej (policja.gov.pl)
https://bielsko-biala.policja.gov.pl/ka2/informacje/wiadomosci/318320,Uwaga-Oszusci-wysylaja-falszywe-linki-wykorzystujac-portal-OLX-oraz-aplikacje-Wh.html

UWAGA NA FAŁSZYWE SMS-Y ZAWIERAJĄCE LINKI DO DOKONANIA PŁATNOŚCI - Świnoujście w sieci www.eswinoujscie.pl
https://www.eswinoujscie.pl/2019/10/15/uwaga-na-falszywe-sms-y-zawierajace-linki-do-dokonania-platnosci/

UWAGA: Oszuści wysyłają fałszywe SMS-y o kwarantannie! - Wiadomości - Komenda Powiatowa Policji w Kłobucku (policja.gov.pl)
https://klobuck.policja.gov.pl/k12/informacje/wiadomosci/321021,UWAGA-Oszusci-wysylaja-falszywe-SMS-y-o-kwarantannie.html

UWAGA: Oszuści wyłudzają dane wysyłają fałszywe e-recepty i informacje o kwarantannie! - Lublin, ESKA.pl
https://www.eska.pl/lublin/falszywe-sms-y-o-kwarantannie-i-e-recepty-aa-LFKS-PMim-WcM4.html

Kliknięcie w link odsyłający do fałszywej strony może doprowadzić do utraty wrażliwych danych uwierzytelniających, tj. haseł i loginów do kont bankowości elektronicznej, poczty email lub mediów społecznościowych. Przez nieuważne kliknięcie można stracić pieniądze, dostęp do ważnych kont, a nawet własną tożsamość. Wykradając nasze poufne dane przestępcy mogą je wykorzystać np. do wyłudzenie pożyczki, zrealizowania transakcji finansowych, czy fałszowania korespondencji.

Statystyka:

Wg. badań jednego z polskich banków – co drugi Polak zetknął się z próbą oszustwa w Internecie.

Najnowsze badania potwierdzają, że przestępstwa w sieci są coraz powszechniejsze i dotyczą również młodszych użytkowników internetu. Już 58 proc. respondentów przyznaje, że oni lub ich bliscy zetknęli się z takimi oszustwami. O tym, jak się przed nimi bronić, bank wyjaśnia w ogólnopolskiej kampanii społecznej.

Dodatkowe źródła informacji:

Co drugi Polak zetknął się z oszustwem w Internecie. Dlatego mBank znów przypomina o bezpieczeństwie w sieci
https://pl.media.mbank.pl/142393-co-drugi-polak-zetknal-sie-z-oszustwem-w-internecie-dlatego-mbank-znow-przypomina-o-bezpieczenstwie-w-sieci#:~:text=Dlatego%20mBank%20zn%C3%B3w%20przypomina%20o%20bezpiecze%C5%84stwie%20w%20sieci,lub%20ich%20bliscy%20zetkn%C4%99li%20si%C4%99%20z%20takimi%20oszustwami.

Tag oszustwa internetowe - Policja.pl
https://www.policja.pl/pol/tagi/323,oszustwa-internetowe.html

Porady, jak rozpoznać FAŁSZYWE STRONY I LINKI?

Nie zawsze jest to proste, ale zachowując kilka podstawowych zasad można samemu sprawdzić, czy strona lub link są prawdziwe.

Uważaj na wszelkie nieoczekiwane wiadomości e-mail i SMS. Cyberprzestępcom łatwo jest sfałszować adres nadawcy nawet w przypadku SMS. Zachowaj czujność zwłaszcza, gdy w wiadomości dostajesz prośbę o kliknięcie w link.

Na czym najczęściej bazują oszuści w sieci? Na naszej ciekawości, pośpiechu, nieuwadze oraz niewiedzy. Zastawiają coraz bardziej wyrafinowane pułapki, w które próbują nas złapać. Jednym ze sposobów, jakie stosują coraz powszechniej, jest tworzenie fałszywych stron internetowych, których głównym celem jest wykradanie naszych danych. Można się jednak przed tym obronić. Trzeba nauczyć się rozpoznawać fałszywe strony, a najłatwiejszym sposobem jest dokładne sprawdzenie ich adresu.

Jak weryfikować adresy www?

Zanim klikniesz w link, dokładnie mu się przyjrzyj, czy dane w nim zawarte faktycznie zawierają adres sugerowanej strony.

Sprawdź czy połączenie na stronie jest szyfrowane. Świadczy o tym adres zaczynający się od **https.** Jeśli strona banku, pośrednika płatności, sklepu, portalu itd. Literka „s" ma tutaj kluczowe znaczenie – oznacza to, że jest to szyfrowana wersja protokołu http. Pamiętaj jednak, że to nie gwarantuje, że strona jest wiarygodna. Informuje nas jedynie o szyfrowaniu danych.

Powiązaną kwestią są certyfikaty. To taki dowód, swoista pieczątka, że dana strona jest bezpieczna. Upewnimy się o tym klikając w ikonę zamkniętej kłódki. Na przykład robiąc to na stronie ipko.pl przeczytamy, że certyfikat jest wystawiony przez PKO Bank Polski i jest ważny. To dowód, że witryna jest prawdziwa i bezpieczna.

Warto także najechać kursorem na link i dokładnie sprawdzić pojawiający się wtedy opis linku – czy rzeczywiście skieruje nas na właściwą stronę , czy też na stronę o podejrzanym adresie.

Kolejną sprawą jest sam adres www – niestety, może on być łudząco podobny do prawdziwego. Na przykład zamiast www.allegro.pl oszuści stworzą www.aIlegro.pl (**ZAUWAŻ**, że zamiast dwóch małych „L" w adresie strony są dwa DUŻE „I" – wyglądają bardzo podobnie, ale ten drugi link skieruje Cię na fałszywą stronę. Kolejny przykład – adres kojarzący się lub przypominający oryginalny - ipko.pl – to oryginalna nazwa, zaś podobną, mając kojarzyć się z oryginałem, można utworzyć w następujący sposób: i-pko.pl, ipkoo.pl albo ipko.bp.pl.

Najważniejsze, żeby za każdym razem, kiedy wchodzimy na strony www, gdzie podajemy swoje dane, dokładnie sprawdzić ich adres, najlepiej litera po literze, cyfra po cyfrze. Jeśli tylko zerkniemy, możemy nie zauważyć drobnych różnic, jak kropki, myślnika czy zestawienia liter (r i n obok siebie, które wyglądają jak „m").[1]

Niestety, im popularniejszy staje się m.in. handel w sieci, tym większą kreatywnością wykazują się nieuczciwi sprzedawcy i cyberprzestępcy. Sposoby ich działania są coraz bardziej wyrafinowane i sprawiające, że każdy powinien zachować czujność i rozwagę w sieci. Jeżeli korzystasz z platformy handlowej, korzystaj jedynie z możliwości komunikowania się z kontrahentami za pośrednictwem narzędzi dostarczanych przez platformę. Jeżeli ktoś proponuje przejście na komunikator lub nietypowe metody płatności czy dostawy, może to być oznaka nieuczciwego działania.

[1] Źródło: https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y

Jeżeli cokolwiek wzbudzi Twoją niepewność, **nie klikaj**, sprawdź, najlepiej sam wpisz adres lub wyszukaj strony, spytaj w prawdziwego dostawcy usługi, czy aby przesłany link jest tym, którego on wysłał.

Dodatkowe źródła wiedzy i dobrych praktyk:

Aktualności - Baza wiedzy - Portal Gov.pl (www.gov.pl)
https://www.gov.pl/web/baza-wiedzy/aktualnosci

Ponad 20 tysięcy niebezpiecznych stron
https://www.gov.pl/web/baza-wiedzy/ponad-20-tysiecy-niebezpiecznych-stron

Tysiące niebezpiecznych stron
https://www.gov.pl/web/baza-wiedzy/tysiace-niebezpiecznych-stron

RAPORT CERT 2020 - Raporty - NASK
https://www.nask.pl/pl/raporty/raporty/4289,RAPORT-CERT-2020.html

CSIRT NASK - NASK
https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html

Bezpieczeństwo w sieci – stosuj zasady i kupuj online (pkobp.pl)
https://bankomania.pkobp.pl/finanse/bezpieczenstwo/zostanwdomu-wykorzystaj-podstawowe-zasady-bezpieczenstwa-w-sieci_2/

Zagrożenia w sieci - fałszywe strony (bitbay.net)
https://bitbay.net/pl/aktualnosci/zagrozenia-w-sieci-falszywe-strony

Bezpieczeństwo. Jak rozpoznać fałszywe strony internetowe. (pkobp.pl)
https://bankomania.pkobp.pl/finanse/bezpieczenstwo/chcesz-zadbac-o-swoje-dane-i-pieniadze-sprawdzaj-adresy-stron-www/

PORADNIK_SKLEPY_CERT_AHS.pdf
https://www.cert.pl/uploads/docs/PORADNIK_SKLEPY_CERT_AHS.pdf

OSZUSTWA INTERNETOWE - JAK SIĘ BRONIĆ? JAK POSTĘPOWAĆ BĘDĄC POKRZYWDZONYM? - Profilaktyka ogólna - KPP Gostyń (policja.gov.pl)
https://gostyn.policja.gov.pl/wl4/profilaktyka/profilatyka-ogolna/182738,OSZUSTWA-INTERNETOWE-JAK-SIE-BRONIC-JAK-POSTEPOWAC-BEDAC-POKRZYWDZONYM.html