Tygodniowe zestawienie

bezpieczeństwa informacji

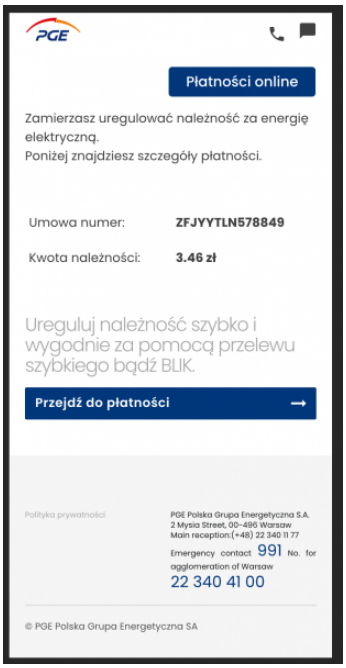
#54

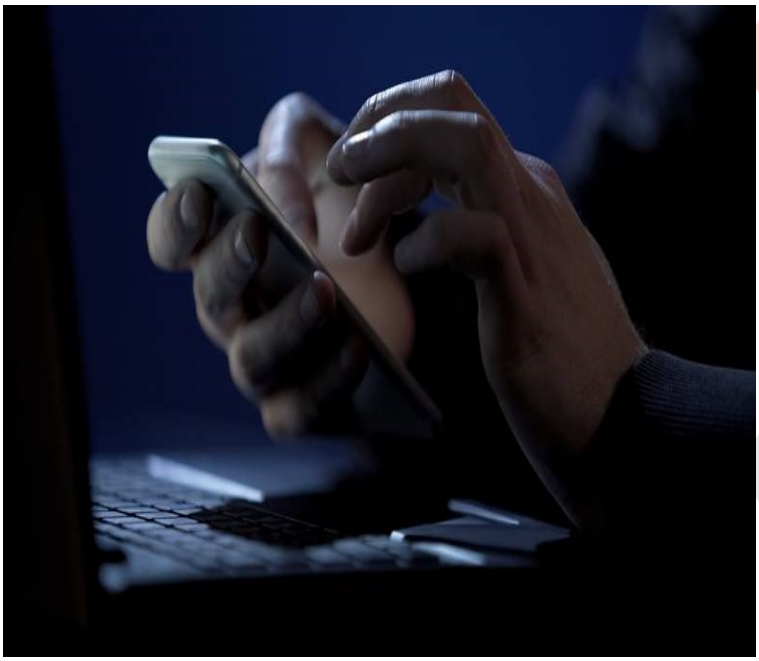
Spis treści

1. Informacje z ostatnich tygodni – krótki opis

1.1. Fałszywe sms-y z PGE?

Po raz kolejny pojawiły się oszustwa w postaci podejrzanych wiadomości podszywających się pod markę PGE próbujących wyłudzić pieniądze. Spółka apeluje do swoich Klientów o szczególną ostrożność i przypomina podstawowe zasady bezpieczeństwa.



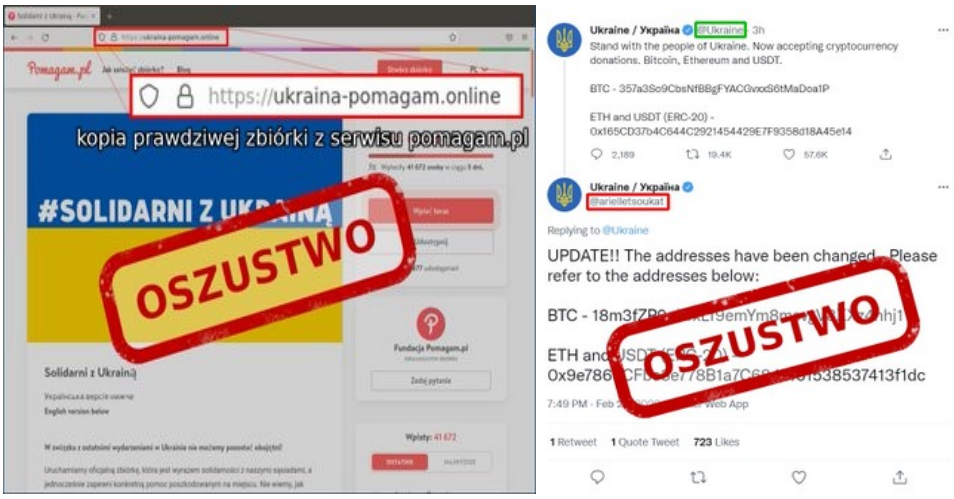


W przesłanej wiadomości znajduje się link, po jego kliknięciu otwiera się strona internetowa przekierowująca do natychmiastowej płatności. W kolejnym kroku hakerzy mogą okraść nas przez BLIK, albo co znacznie poważniejsze, pozyskają dane służące do nieograniczonego dostępu do środków finansowych na naszym koncie.

Przejdź do artykułu źródłowego: https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/dostales-sms-z-pge-o-platnosci-za-prad-uwaga-mozna-stracic-pieniadze/8g59xdw

1.2. Fałszywe zbiórki pieniędzy na pomoc Ukrainie

Obecna sytuacja toczącej się wojny na Ukrainie spowodowała iż organizowane są liczne zbiórki pomocy dla Ukrainy i jej obywateli. W tym celu zostały zorganizowane różne aukcje. Niestety fakt ten wykorzystywany jest również przez oszustów. CERT Polska i zespół ds. cyberbezpieczeństwa CSIRT działający przy KNF ostrzegają przed tego rodzaju oszustwami.



Wykorzystując prawdziwą aukcję ze strony Pomagam oszuści podmienili numery rachunków bankowych do wpłat. Drugi przykład powiązany jest z dotacjami poprzez kryptowaluty.

Rozsyłane mogą być również wiadomości e-mail, z prośbą o wsparcie obywateli Ukrainy poprzez przekazy pieniężne. Przykład takiego maila został zamieszczony przez zespół ds. cyberbezpieczeństwa CSIRT na swoim profilu w mediach społecznościowych.


Yurri Shevchenko <yurrishevchenko5@gmail.com>
Cześć

Cześć,

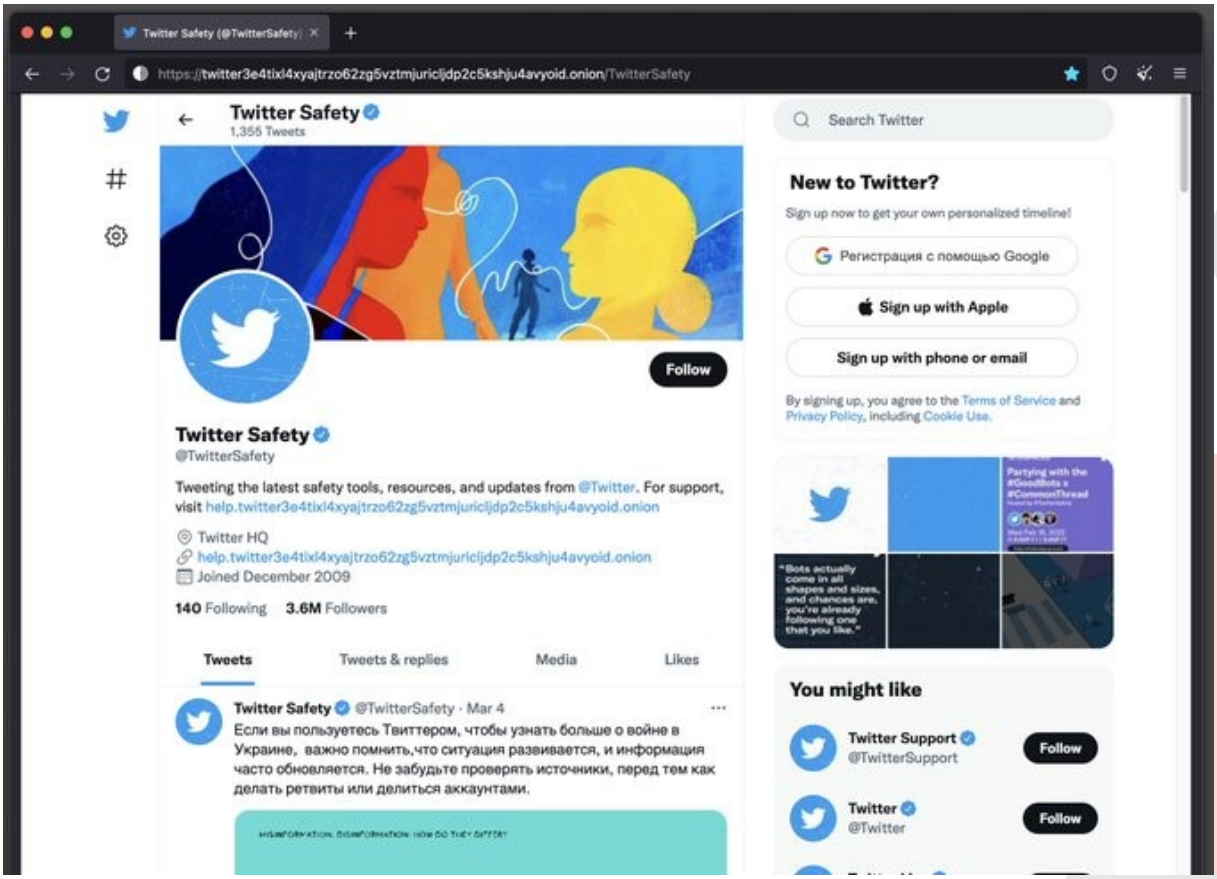
Przepraszamy za niedogodności, jakie może spowodować moja wiadomość. Powiem krótko, jestem inżynierem okrętowym z rządem ukraińskim zaangażowanym w obecną wojnę z Rosją. Stacjonuję w podziemnej stacji wojskowej w Charkowie i czekam na planowany przez naszego goryla atak na najeźdźców rosyjskich. Proszę pozwolić mi poprosić o pomoc w przeprowadzce mojej trzysobowej rodziny do twojego kraju ze względów bezpieczeństwa. Nie mogę już nic zrobić z naszej kryjówki z powodu ciężkiego ostrzału wojsk rosyjskich. W obecnej formie pomoc, o którą proszę, polega na pomocy mojej żonie i dzieciom w wyprowadzce się drogą dyplomatyczną do twojego kraju i zainwestowaniu naszego miliona euro w gotówkę w rentowny, lukratywny obszar, który przyniesie większe zyski zamiast go stracić . Obecnie mogę wysyłać e-maile tylko z podziemia, a ryzyko jest zbyt duże, aby być stale online. Nasze rodzinne pieniądze są w zapieczętowanej skrzynce bezpieczeństwa, którą tylko ja znam kody dostępu do jej otwarcia. Moja żona nawet nie wie, że jest tam z nią, ponieważ powiedziałem jej, że to biżuteria, jedyne, czego potrzebuję, to skontaktowanie się z nią i poprowadzenie ich, aby bezpiecznie ćwiczyli. Mam pieniądze, ale nie mogę ich ruszyć, dlatego trzeba natychmiast opuścić z nimi Ukrainę. Dalsze informacje przyjdą po otrzymaniu wiadomości od Ciebie, proszę o wszelkie pytania.

Przed wpłaceniem środków pieniężnych, ważne jest sprawdzenie wiarygodności zbiórki.

Przejdź do artykułu źródłowego: https://bezprawnik.pl/falszywe-zbiorki-pieniedzy-dla-ukrainy/; https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/uwaga-na-falszywe-zbiorki-dla-ukraincow-oszusci-chca-was-okrasc/bg0g6p9

1.3. Twitter w sieci TOR

Z oficjalnego konta The Tor Project dowiadujemy się działaniu Twittera w sieci Tor. Została uruchomiona specjalna wersja do której da się dotrzeć w sieci Tor. Chodzi o wirtualną sieć z mechanizmami zapobiegającymi śledzeniu, gdyż nie ma tu możliwości jakiejkolwiek analizy ruchu. Tor pozwala korzystać z sieci anonimowo. W dobie wojny z Ukrainą może mieć to szczególne znaczenie, gdyż Rosjanie zostali już odcięci od Facebooka i Twittera co miało uniemożliwić im dostęp do prawdziwych informacji o wojnie. Twitter działający w Torze może być więc drogą dostępu Rosjan do niepropagandowych treści.

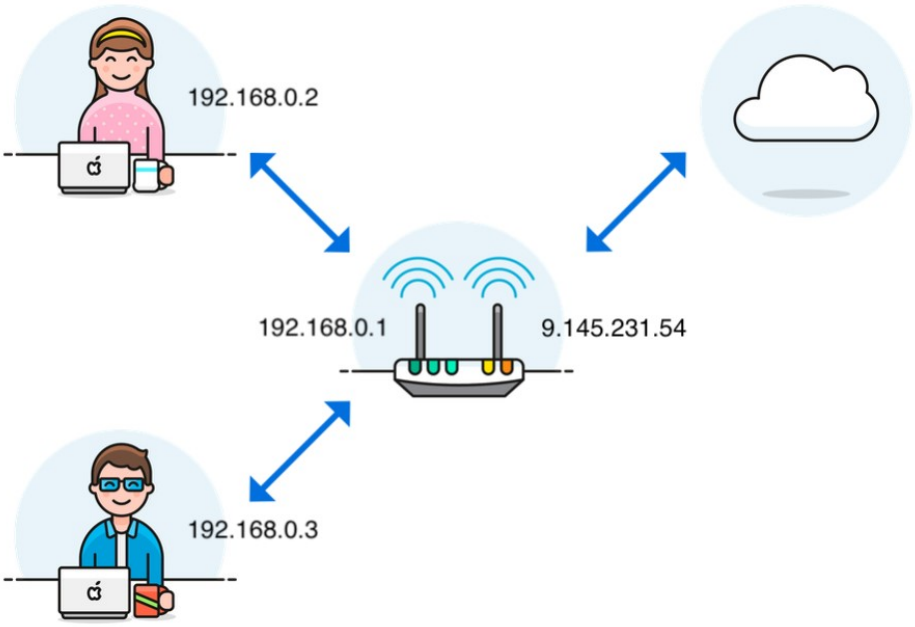


Przejdź do artykułu źródłowego: https://www.dobreprogramy.pl/twitter-dziala-w-sieci-tor-wrotach-do-podziemia-internetu,6745400151841376a

2. Zalecenia i dobra praktyka według “bezpieczników”

2.1. Jak poprawnie skonfigurować domowy router

W artykule z dnia 23 lutego 2022 roku „Sekurak” umieścił kilka rad jak poprawnie i bezpiecznie skonfigurować domowego routera. Pierwszym pytaniem na które należy sobie odpowiedzieć jest czy warto zaopatrzyć się we własny router? Przy połączeniu przekazanego przez operatora urządzenia tzw. modemu z internetem poprzez sieć Wi-Fi bądź przy użyciu kabla sieciowego może dojść do braku kontroli nad urządzeniem, braku aktualizacji a także wycieku defaultowych poświadczeń. Między innymi dlatego też z tych względów warto zaopatrzyć się we własny router. W modemie można wtedy wyłączyć wszystkie usługi, co daje nam dodatkową korzyść z takiej konfiguracji czyli ukrycie naszego routera za urządzeniem od operatora, co utrudni ataki z Internetu.



W dalszej części artykułu przedstawiono o czym należy pamiętać przy konfiguracji routera.

Przejdź do artykułu źródłowego: https://sekurak.pl/o-czym-pamietac-konfigurujac-bezpieczenstwo-domowego-routera-wifi/

2.2. Rosyjskie programy i dystrybucje

W swojej publikacji Andrzej Tarnowski na stronie ”dobreprogramy.pl” przedstawia kilka programów i dystrybucji rosyjskich, z których nie wypada już korzystać. Są wśród nich programy antywirusowe oraz dystrybucje linuksowe, a także rosyjsko-holenderska przeglądarka internetowa.

Wśród najpopularniejszych rosyjskich programów antywirusowych możemy znaleźć Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky Safe Kids.

Do najbardziej znanych rosyjskich dystrybucji linuksowych należy natomiast: ALT Linux, ROSA Linux, Calculate Linux oraz Astra Linux. Do najbardziej popularnej przeglądarki internetowej w Rosji należy natomiast Yandex.

Przejdź do artykułu źródłowego https://www.dobreprogramy.pl/@antar/rosyjskie-programy-i-dystrybucje-z-ktorych-nie-wypada-juz-korzystac,blog,115705