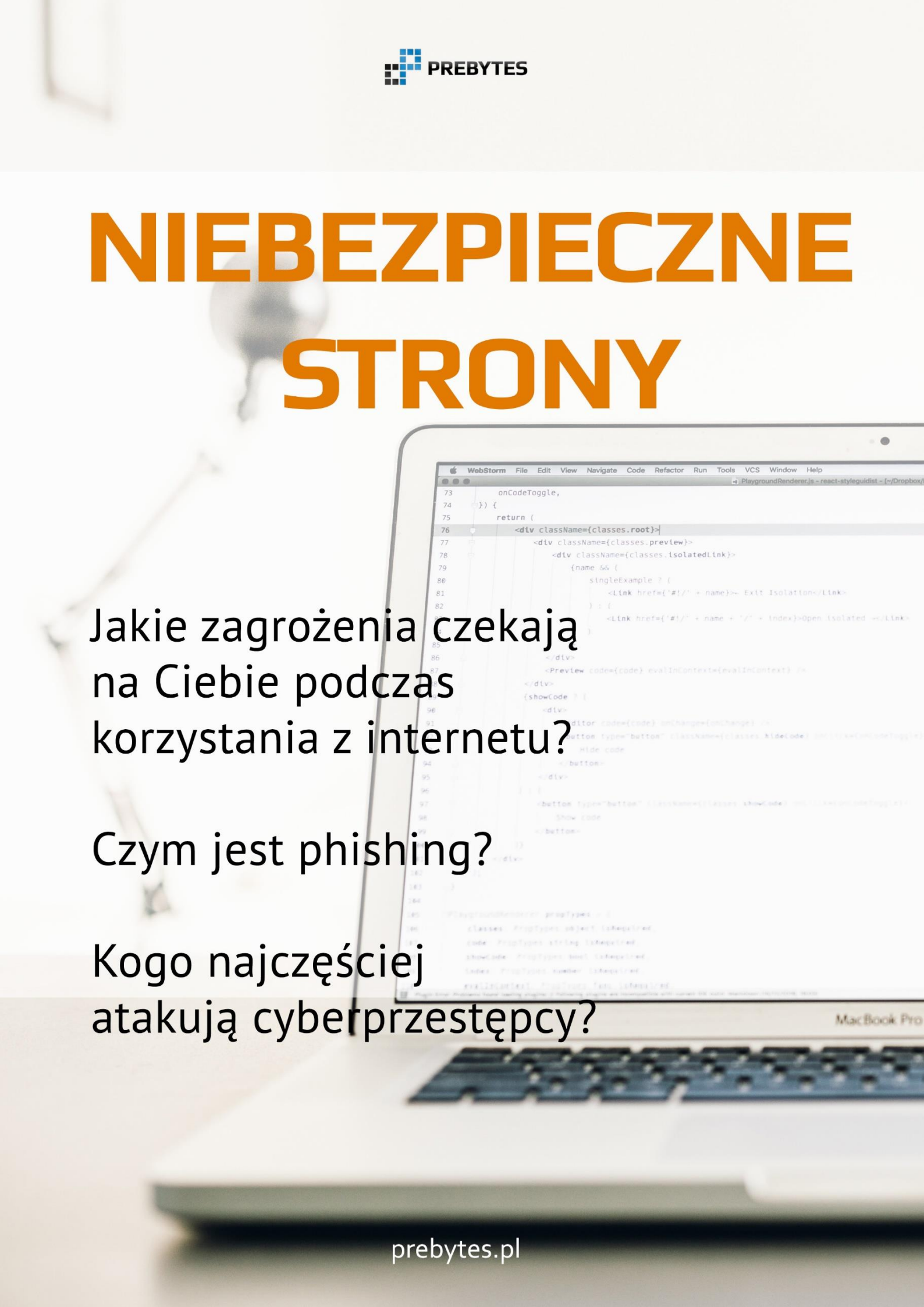
PREBYTES

NIEBEZPIECZNE STRONY



Jakie zagrożenia czekają na Ciebie podczas korzystania z internetu?

Czym jest phishing?

Kogo najczęściej atakują cyberprzestępcy?

Spis treści

Wprowadzenie 1
Jak niebezpieczny jest spam? 2
Phishing 3
Na czym polega atak phishing? 4
Phishing w liczbach 5
Tematy wiadomości 6
Niebezpieczna wiadomość – nie daj się oszukać! 7
Strona phishingowa – jak ją rozpoznać? 9
Phishing w mediach społecznościowych 10
Ile warte są wizerunki znanych marek? 11
Świeć przykładem – praktyczne porady 12
Kalendarium 2017 13

Niebezpieczne strony

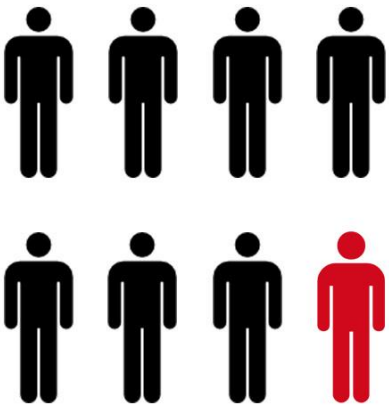
Jakie zagrożenia czekają na Ciebie podczas korzystania z internetu?

Wprowadzenie

Z roku na rok w Polsce rośnie liczba gospodarstw domowych ze stałym dostępem do internetu. Tym samym wzrasta liczba osób regularnie korzystających z internetu. Każdego dnia na całym świecie wysyłanych jest wiele milionów wiadomości email. Jak wynika z danych Głównego Urzędu Statystycznego, Polacy najczęściej używają internetu właśnie po to, aby skorzystać z poczty elektronicznej. Większość z nas ufa, że źródło, z jakiego pochodzi przysłana do nas wiadomość jest bezpieczne. Nie sprawdzamy dokładnie adresu email nadawcy i nie zwracamy uwagi na otrzymywane w wiadomościach załączniki. Z naszej nieuwagi coraz częściej korzystają cyberprzestępcy. Wykorzystują oni naszą naiwność po to, aby okraść nas z poufnych danych, a w rezultacie przejąć nasze pieniądze.

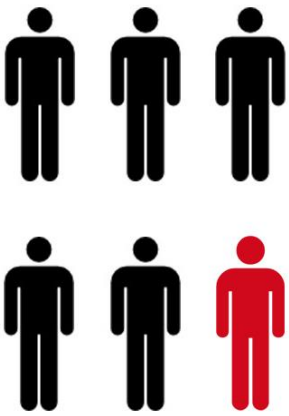
80% **Polaków ma dostęp do internetu***

Jedna na osiem osób otwiera niebezpieczną stronę.



60% **Użytkowników internetu korzysta z poczty elektronicznej***

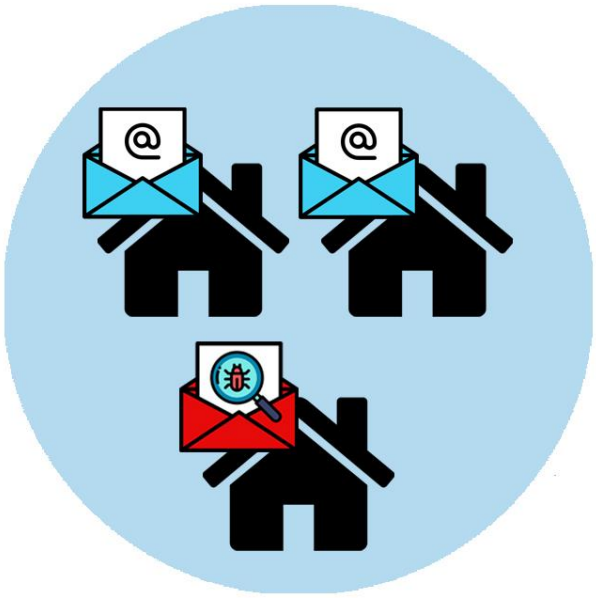
Znajdujesz się w grupie osób, które codziennie otrzymują wiadomości od cyberprzestępców.



*) źródło: GUS, stat.gov.pl (2016)

Jak niebezpieczny jest spam?

Masowo rozsyłane wiadomości email, tzw. spam są nieodłącznym narzędziem ataku stosowanym przez cyberprzestępców. Kampania spamowa jest sposobem na bardzo szeroką dystrybucję wiadomości, które zawierają odnośniki do stron wyłudzających poufne dane, m.in. loginy i hasła lub dane kart debetowych i kredytowych. Przy pomocy specjalnych technik manipulacji, spamerzy przekonują odbiorcę wiadomości do uruchomienia załącznika lub wizyty na określonej stronie internetowej.



1 na 3

gospodarstwa domowe

z dostępem do internetu jest narażone na otrzymywanie wiadomości spam.

To właśnie Ty mogłeś zostać ofiarą ataku cyberprzestępców i stracić oszczędności życia.



20 mln

wiadomości spamowych zostało wykrytych od maja do grudnia 2017 roku



76%

wiadomości spam jest rozsyłanych w dni robocze



9^{00} - 16^{00}

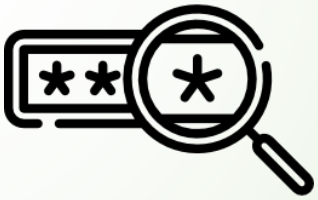
w tych godzinach rozsyłanych jest najwięcej wiadomości spamowych

*) źródło: PREBYTES Security Incident Response Team (2017)



Phishing

Phishing jest oszustwem polegającym na podszywaniu się pod legalnie działające organizacje lub osoby prywatne, w celu wyłudzenia poufnych danych.



Phishing obejmuje kradzież numerów kart kredytowych i debetowych, haseł dostępu do bankowości elektronicznej i serwisów internetowych oraz innych poufnych danych.



Phisher to osoba, która za pośrednictwem internetu przechwytuje poufne dane użytkowników i wykorzystuje je w swojej przestępczej działalności.



Na czym polega atak phishing?



Cyberprzestępca podszywając się pod znaną firmę lub osobę wysyła wiadomość, która zawiera nieprawdziwą treść oraz odnośnik do strony wyłudzającej poufne dane (phishing).



Potencjalna ofiara otwiera wiadomość i klika w załączony do niej odnośnik, który natychmiast przekierowuje ją do strony wyłudzającej poufne dane.



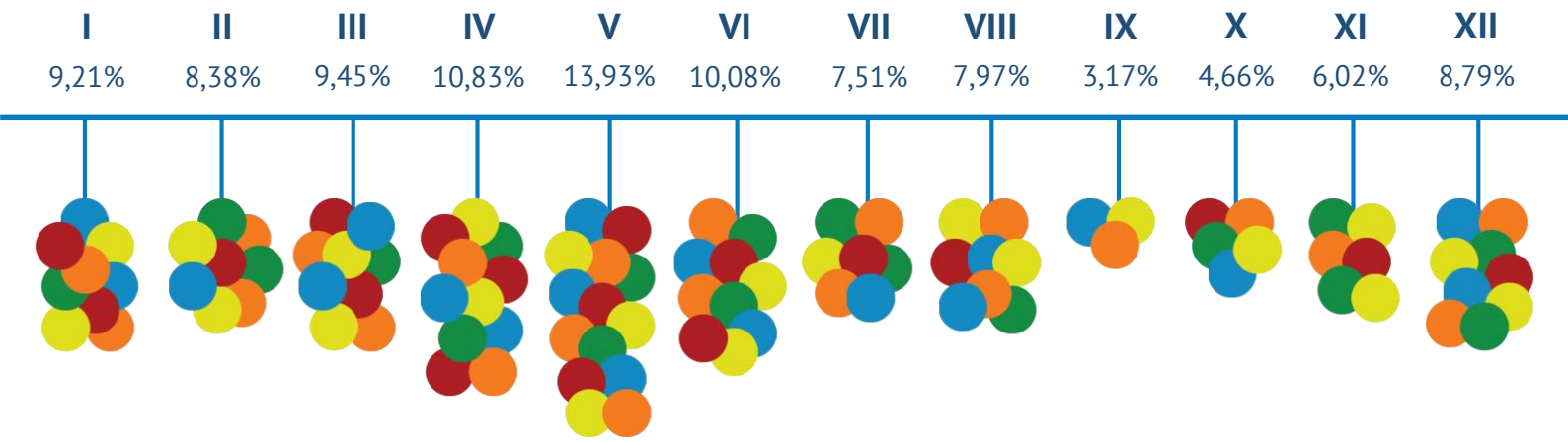
Otwarta strona phishing swoim wyglądem przypomina oryginalną stronę wybranej organizacji lub banku. Użytkownik zawsze proszony jest o podanie na niej poufnych danych.



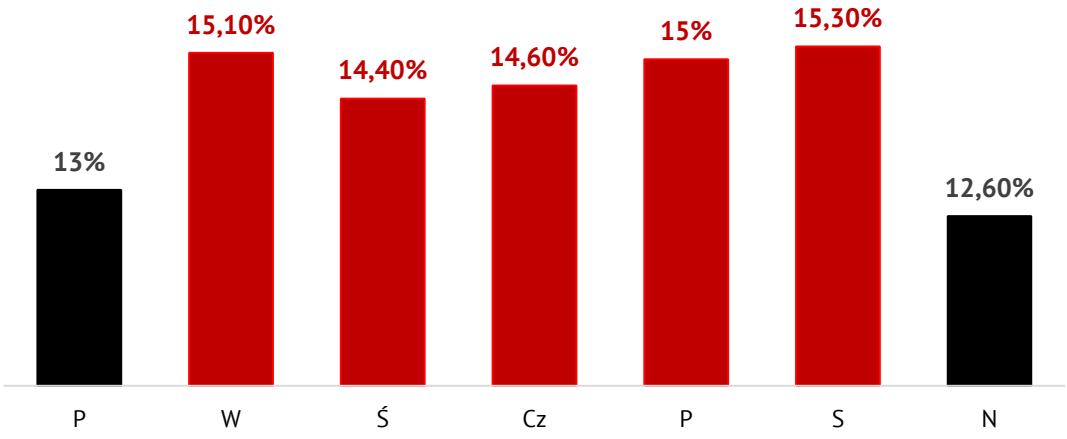
Podane przez użytkownika dane natychmiast trafiają do **phishera**, który wykorzystuje je, aby uzyskać dostęp do konta bankowego swojej ofiary i wypłacić z niego pieniądze.

Phishing w liczbach

Intensywność ataków w 2017 roku



Ataki phishing w poszczególne dni tygodnia



Cyberprzestępcy masowo rozsyłają wiadomości spam, zawierające linki do specjalnie stworzonych przez nich stron, wyłudzających poufne dane. Im więcej fałszywych wiadomości zostanie wysłanych, tym wyższe jest prawdopodobieństwo, że większa ilość osób otworzy otrzymanego emaila, kliknie w załączony link, który przekieruje ją do strony phishing i poda przestępcy swoje dane.

Najwięcej ataków phishing ma miejsce w godzinach

$14^{00} - 17^{00}$



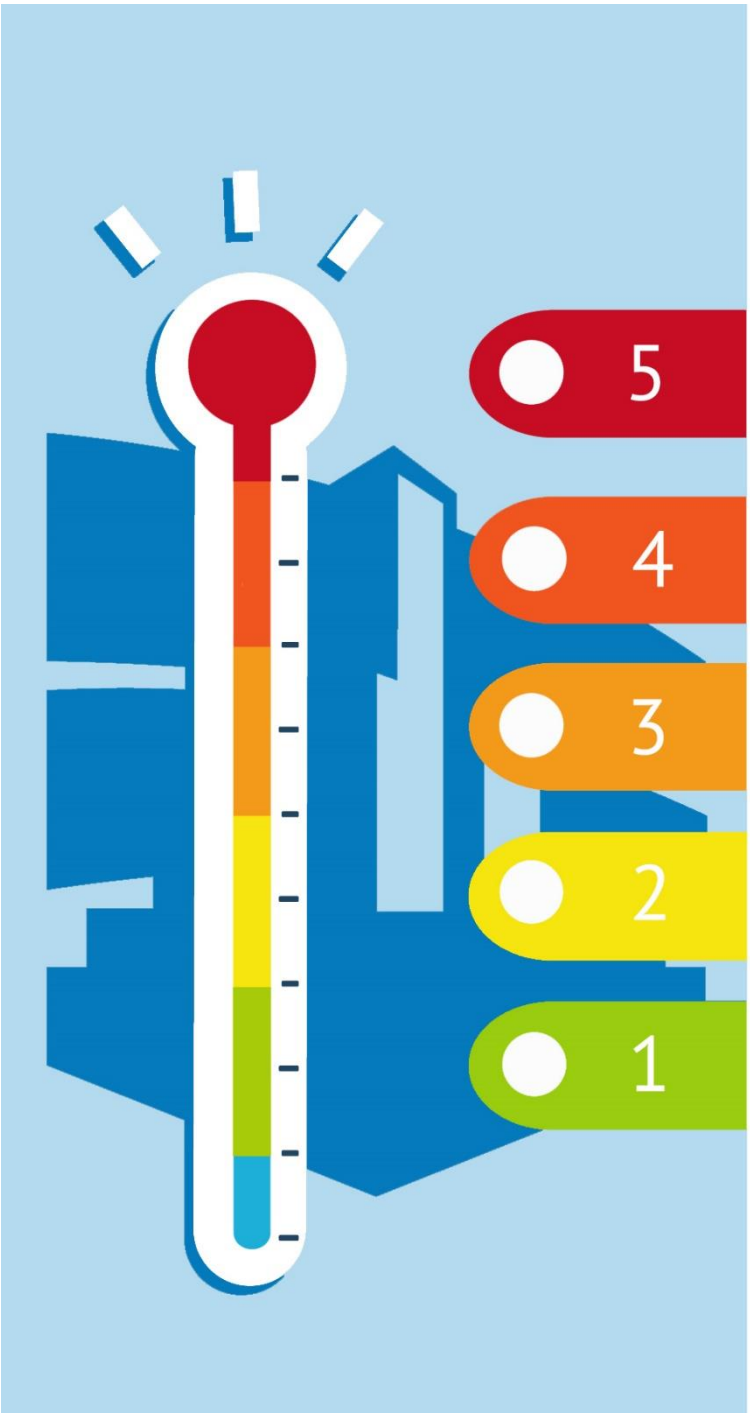
Tematy wiadomości

Temat otrzymanej wiadomości zwykle jest interesujący i ma wywołać u odbiorcy natychmiastowe zaciekawienie i jej otwarcie. Tematy zwykle oznajmiają, że wiadomość zawiera informacje o otrzymanej fakturze, dokonanym zakupie, wysłanej lub zaginionej przesyłce, dokonanym rozliczeniu, czy nadpłacie. Cyberprzestępcy często w tematach wysyłanych wiadomości umieszczają nazwę banku lub innej organizacji. W ten sposób zwiększają prawdopodobieństwo, że odbiorca uwierzy w autentyczność otrzymanego emaila i da się oszukać.



Niebezpieczna wiadomość – nie daj się oszukać!

Wiadomości spam mogą zawierać wymyślone historie, ale najczęściej przybierają formę fałszywych powiadomień z różnych organizacji oraz banków. Przestępcy zwykle proszą w nich o zatwierdzenie, zaktualizowanie danych lub informują o pewnych nieprawidłowościach. Treść wiadomości ma wzbudzić niepokój i skłonić odbiorcę do kliknięcia w załączony odnośnik do strony internetowej. Wiadomości od cyberprzestępców zawierają informacje, które mają za zadanie nakłonić nas do kliknięcia w otrzymany link. W przeciwnym razie, nasze konto bankowe zostanie NIEODWRACALNIE zablokowane a dane zostaną NA ZAWSZE usunięte.



Cyberprzestępca zdobywa u Ciebie punkty zaufania. Im więcej ich zbierze, tym większe jest prawdopodobieństwo, że podasz mu swoje dane.

5 — Otwarcie przez Ciebie linku przekierowującego do fałszywej strony jest dla przestępcy prawdziwym sukcesem. — REALNE ZAGROŻENIE

4 — Prawdziwe dane organizacji tylko utwierdzają Cię w przekonaniu, że treść wiadomości jest prawdziwa.

3 — Treść wiadomości, która Cię zainteresuje, to już dla przestępcy połowa sukcesu.

2 — Temat, który skłoni Cię do otwarcia wiadomości, zwiększa szanse przestępcy na skuteczny atak.

1 — Nadawca wiadomości, na którego zwrócisz uwagę jest dla przestępcy pierwszym krokiem do osiągnięcia sukcesu.

MANIPULACJA

Nadawca wiadomości często jest wyświetlany jako nazwa zaufanej organizacji lub czyjeś imię i nazwisko.

Temat ma nas zaniepokoić, nakłonić do natychmiastowego odczytania wiadomości.

Najwięcej stron phishing otwieranych jest w pierwszych **3 godzinach** od otrzymania spamu



Warto zwrócić uwagę na błędy, które mogą wystąpić w treści wiadomości. Cyberprzestępcy atakujący w innym języku często popełniają błędy ortograficzne oraz stylistyczne.

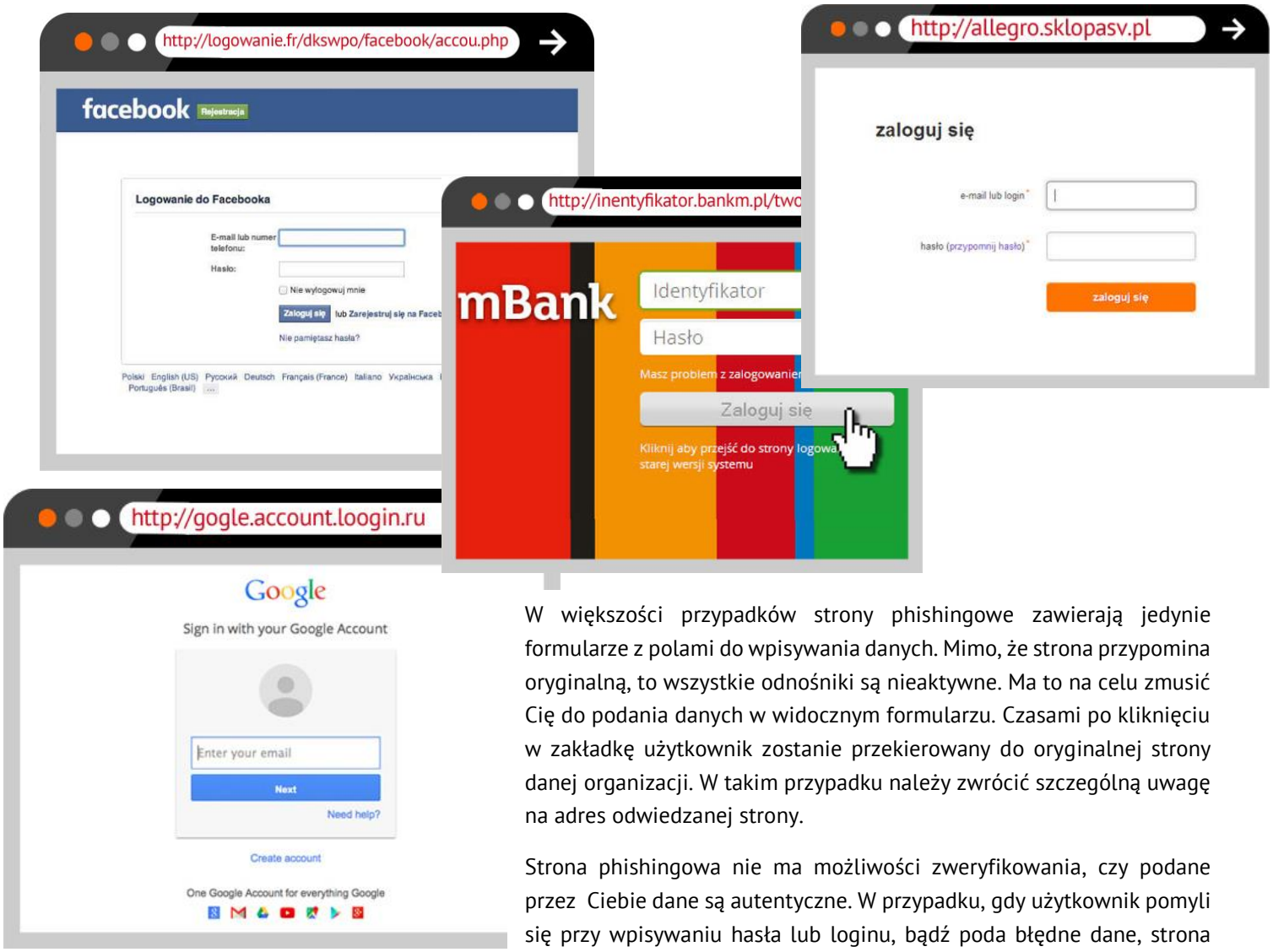
Cyberprzestępcy bardzo często w wysyłanej wiadomości podają prawdziwe **dane kontaktowe** instytucji, pod jaką się podszywają.

Treść wiadomości zawiera niepokojący komunikat, np. o blokadzie konta w banku, zaginionej przesyłce, itp.

REALNE ZAGROŻENIE!

Link zawiera odnośnik do strony phishing, gdzie użytkownik będzie proszony o podanie poufnych danych.

Strona phishing – jak ją rozpoznać?



W większości przypadków strony phishingowe zawierają jedynie formularze z polami do wpisywania danych. Mimo, że strona przypomina oryginalną, to wszystkie odnośniki są nieaktywne. Ma to na celu zmusić Cię do podania danych w widocznym formularzu. Czasami po kliknięciu w zakładkę użytkownik zostanie przekierowany do oryginalnej strony danej organizacji. W takim przypadku należy zwrócić szczególną uwagę na adres odwiedzanej strony.

Strona phishingowa nie ma możliwości zweryfikowania, czy podane przez Ciebie dane są autentyczne. W przypadku, gdy użytkownik pomyli się przy wpisywaniu hasła lub loginu, bądź poda błędne dane, strona phishingowa nie rozpozna tego. W konsekwencji nie pojawi się komunikat o niepoprawnie wpisanym haśle lub loginie, jaki pojawiłby się na oryginalnej stronie.

Po wprowadzeniu poufnych danych, strony phishingowe zwykle nie logują użytkowników do serwisu, pod jaki się podszywają. Zazwyczaj pojawia się komunikat o tym, że witryna wygasła, logowanie jest błędne, czy w serwisie prowadzone są prace modernizacyjne. Zdarzają się jednak bardzo dobrze przygotowane ataki phishing, gdzie po podaniu swoich danych, użytkownik jest logowany do autentycznej witryny.



Strona phishing atakuje średnio przez 20 godzin*

*) źródło: APWG, apwg.org

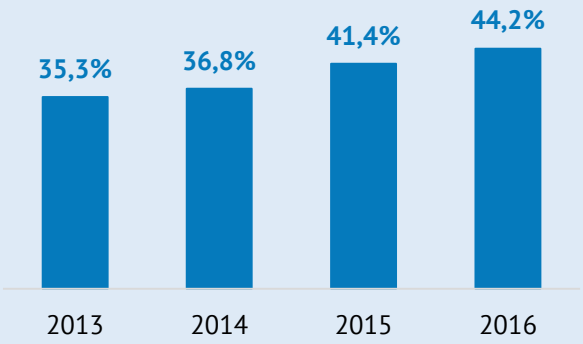
Strona phishing zawsze

1. Ma inny adres, niż oryginalna strona.
2. Posiada pole do wpisywania poufnych danych.

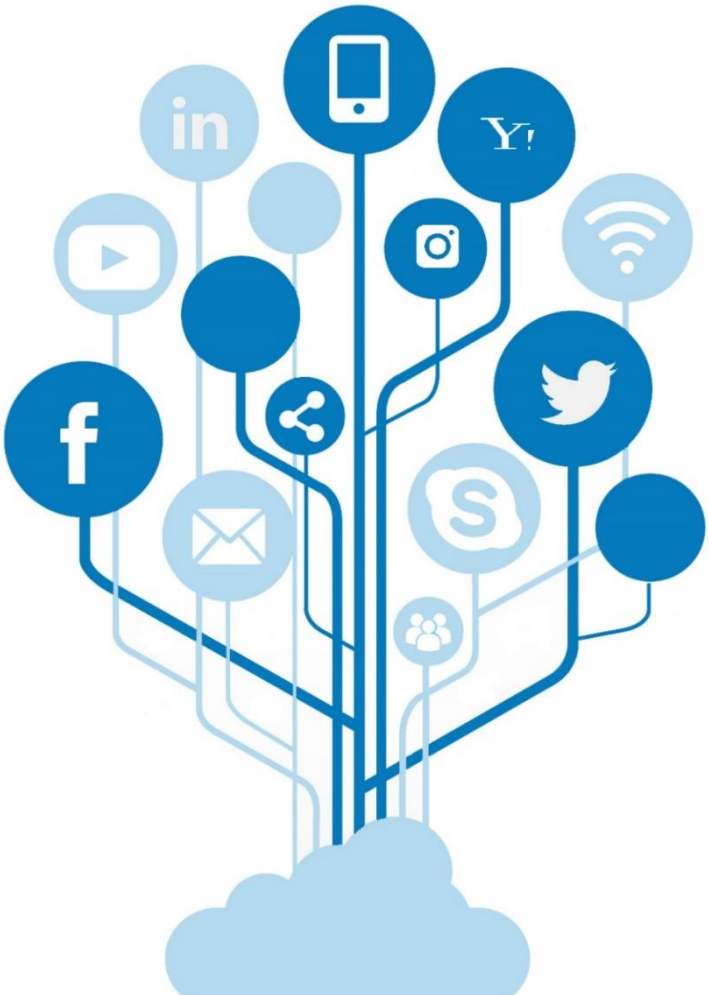
Phishing w mediach społecznościowych

W obecnych czasach pocztę elektroniczną częściowo zastępują media społecznościowe, przy pomocy których użytkownicy internetu mogą komunikować się między sobą. Niestety świadomość zagrożeń, na jakie mogą być narażeni użytkownicy, korzystający z tych portali wciąż pozostaje bardzo niska. Użytkownikowi portalu społecznościowego zazwyczaj wydaje się, że przestępcy nie osiągną żadnych korzyści uzyskując dostęp do jego konta, a on sam nie ma nic do stracenia. Mało kto zdaje sobie sprawę, że przechwycone przez przestępcę konto jest pośrednikiem w jego przestępczej działalności i służy mu głównie do oszukiwania kolejnych osób.

Korzystanie z serwisów społecznościowych w Polsce
osób w wieku 16-74 lat



źródło: GUS, stat.gov.pl



Cyberprzestępcy uzyskując dostęp do konta na portalu społecznościowym wysyłają z niego wiadomości do znajomych swojej ofiary. Poszerzają oni w ten sposób swoją bazę kontaktów i mogą wysyłać więcej fałszywych wiadomości, pozyskując tym samym kolejne ofiary. Użytkownicy portali społecznościowych z reguły ufają swoim znajomym i otrzymując wiadomość od znajomego zwykle wierzą, że jest ona bezpieczna i nie ma w niej złośliwych treści. Ludzie znacznie chętniej klikają w załączniki lub linki otrzymywane w wiadomościach od swoich przyjaciół lub organizacji, z którymi są połączeni na portalu, niż od osób nieznajomych. Metoda ta jest znacznie skuteczniejsza, niż rozsyłanie spamu z fałszywych, nieznanych nikomu kont.

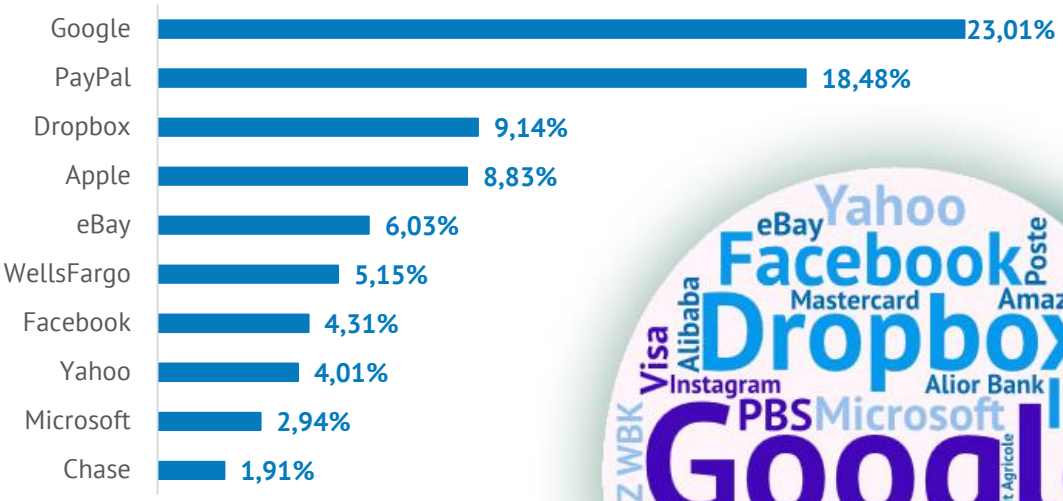
Twoje konto na portalu społecznościowym
nie jest bezpieczne.

Cyberprzestępcy przy jego pomocy mogą
okraść Twoich znajomych.

Ile warte są wizerunki znanych marek?

Znaczna część wiadomości phishing podszywa się pod legalnie działające organizacje. Najczęściej atakowanymi instytucjami są systemy płatności online, sklepy internetowe, banki oraz serwisy społecznościowe.

TOP 10 atakowanych instytucji







Ataki cyberprzestępców są niebezpieczne nie tylko dla klientów korzystających z usług znanych marek. Działają również na szkodę organizacji, których wizerunki są wykorzystywane. Klienci mogą stracić do nich zaufanie i w rezultacie zniechęcić się do korzystania z ich usług lub nawet całkiem z nich zrezygnować.

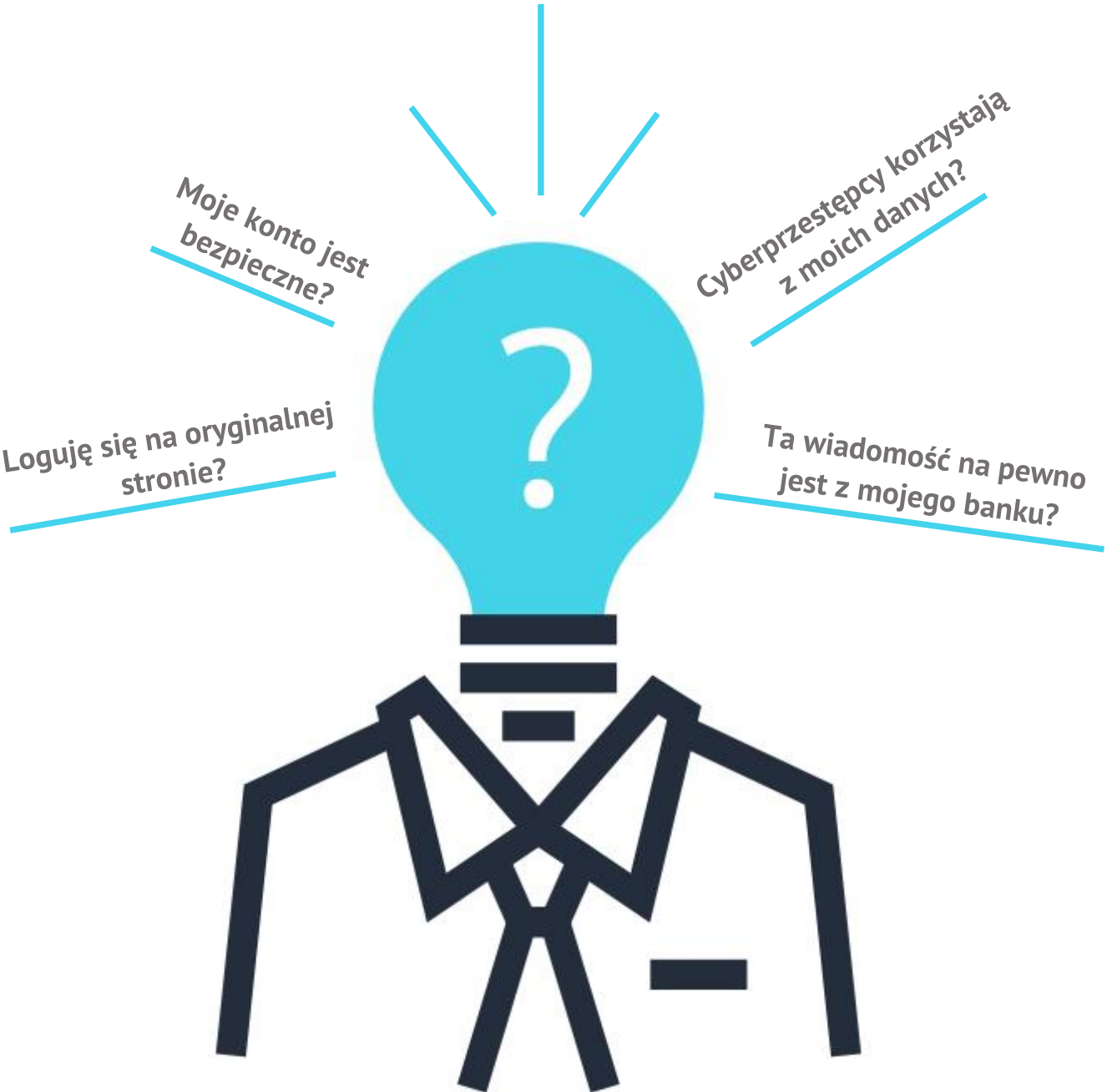
Świeć przykładem – praktyczne porady

1. Nawet, gdy przez przypadek lub chwilową nieuwagę znajdziesz się na stronie phishing – nie podawaj żadnych danych! Samo otwarcie strony, bez podawania jakichkolwiek informacji zazwyczaj nie pociąga za sobą żadnych poważnych konsekwencji.

2. Gdy po podaniu hasła zauważysz, że coś jest nie tak (nie zostałeś zalogowany, witryna wygasła), natychmiast je zmień.

3. W przypadku otrzymania wiadomości phishing, zgłoś to na **zglosincydent.pl** i poinformuj organizację, której wizerunek jest wykorzystywany.

4. Pamiętaj, że bank nigdy nie prosi Cię o podanie poufnych danych w wiadomości email lub przez telefon.



Kalendarium 2017

Styczeń

Podszywając się pod policję przestępcy wyświetlali fałszywe komunikaty o blokadzie komputera, w celu wymuszenia grzywny.

Luty

Przestępcy podając się za pracowników portalu OLX dzwonili do użytkowników, od których próbowali wyłudzić poufne dane.

Marzec

Przestępcy prowadzili kampanię phishing, ukierunkowaną na największe banki w Polsce.

Kwiecień

Rozsyłane były wiadomości spam, podszywające się pod Multimedia Polska z załączoną eFakturą.

Maj

Przestępcy wyłudzali dane do bankowości elektronicznej, za pośrednictwem portalu aukcyjnego Allegro.

Czerwiec

Prowadzona była kampania phishing, ukierunkowana na systemy płatności online, w szczególności na PayU.

Lipiec

Przestępcy wyłudzali pieniądze przy użyciu fałszywej strony, podszywającej się pod fundację SiePomaga.

Sierpień

Podszywając się m.in. pod płatności online Skrill, przestępcy wyłudzali poufne dane.

Wrzesień

Przestępcy w adresach fałszywych stron wykorzystywali nazwę usługi pay-by-link.



Październik

Fala masowych ataków phishing na platformy bankowości elektronicznej, w których przestępcy wykorzystywali logotyp Dotpay.

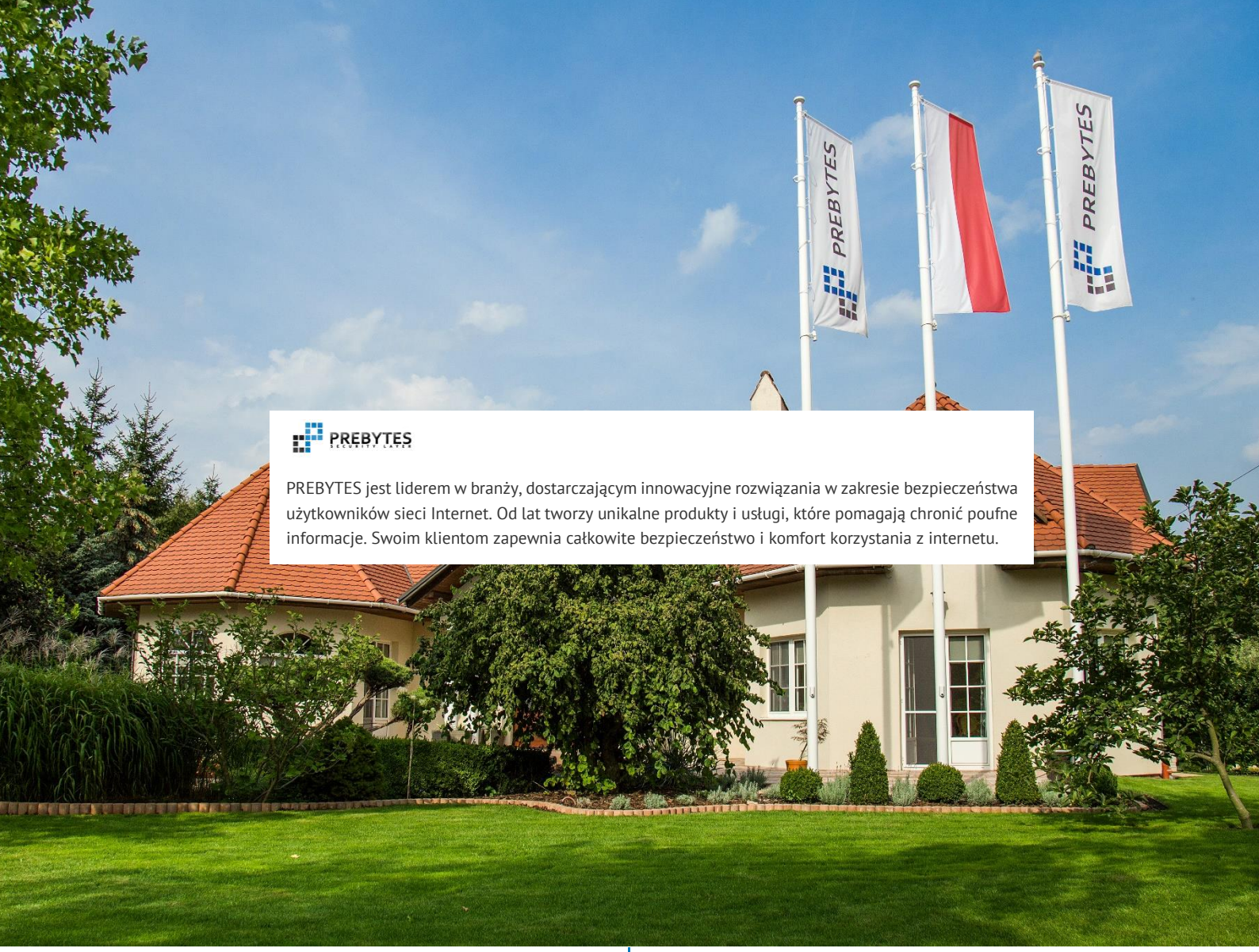
Listopad

Cyberprzestępcy stworzyli stronę wyłudzającą dane logowania z uniwersalnym formularzem dla wszystkich bankowości online.



Grudzień

Zaobserwowano aktywność przestępców na forach, gdzie rekrutowali osoby do współpracy przy atakach phishing.



PREBYTES jest liderem w branży, dostarczającym innowacyjne rozwiązania w zakresie bezpieczeństwa użytkowników sieci Internet. Od lat tworzy unikalne produkty i usługi, które pomagają chronić poufne informacje. Swoim klientom zapewnia całkowite bezpieczeństwo i komfort korzystania z internetu.

https://www.facebook.com/PREBYTES/
https://www.facebook.com/PREBYTES.SIRT/

https://twitter.com/PREBYTES
https://twitter.com/PREBYTES_SIRT

https://prebytes.pl
https://sirt.pl

ul. Sandomierska 6, 37-300 Leżajsk, Polska
+48 (17) 785 19 85
hello@prebytes.pl

W przypadku wykrycia aktywnego zagrożenia zgłoś to ekspertom z PREBYTES SIRT.

https://zglosincydent.pl

Copyright © 2018 Prebytes. All rights reserved.

Wszelkie informacje w tym dokumencie mogą ulec zmianie bez uprzedniej informacji oraz są przedstawione na zasadach „TAKIE JAKIE JEST" (AS IS).

PREBYTES nie udziela absolutnie żadnych gwarancji – całościowych lub/oraz częściowych na wszystkie informacje tekstowe, obrazkowe oraz binarne. PREBYTES dokłada wszelkich starań, aby dane zawarte w raporcie były kompletne, aktualne i zgodne ze stanem faktycznym, nie może tego jednak zagwarantować i w związku z tym faktem nie ponosi żadnej odpowiedzialności za skutki wykorzystywania prezentowanych danych, w szczególności za szkody powstałe w wyniku korzystania z nich. W żadnym wypadku PREBYTES nie ponosi odpowiedzialności za wszelkie skutki lub szkody, w tym bezpośrednie, pośrednie, przypadkowe, wynikowe, utratę zysków handlowych lub szkody specjalne, wynikające z lub w związku z używaniem lub rozpowszechnianiem informacji zawartych w niniejszym raporcie.

Zabronione jest wykorzystywanie niniejszego raportu do świadczenia usług naruszających prawa PREBYTES, o ile zawarta umowa nie stanowi inaczej. Dystrybucja niniejszego dokumentu wymaga pisemnej zgody PREBYTES.

Wszelkie zarejestrowane i niezarejestrowane znaki towarowe użyte w tym dokumencie są własnością ich właścicieli.