NIEODPŁATNE USŁUGI
-POMOC PRAWNA
-PORADY OBYWATELSKIE
-MEDIACJA

Ministerstwo Sprawiedliwości

sursum corda STOWARZYSZENIE w górę serca

E-INFORMATOR PRAWNY

OSZUSTWA INTERNETOWE

PHISHING I FAŁSZYWE OFERTY

- CZYM JEST PHISHING
- JAK ROZPOZNAĆ OSZUSTWO
- JAK SIĘ CHRONIĆ

NP.MS.GOV.PL | POMOCPRAWNA.SC.ORG.PL

SYSTEM NIEODPŁATNEJ POMOCY W POLSCE

Nieodpłatna pomoc to gwarancja, że każdy - niezależnie od sytuacji życiowej i materialnej - może uzyskać rzetelną informację prawną oraz wsparcie w rozwiązaniu swoich problemów. **To prawo każdego z nas** - finansowane ze środków publicznych.

Z JAKIEJ POMOCY MOŻESZ SKORZYSTAĆ?

Nieodpłatna Pomoc Prawna

Uzyskasz informację prawną, wyjaśnienie przepisów oraz pomoc w przygotowaniu pism, wniosków i oświadczeń.

Nieodpłatne Poradnictwo Obywatelskie

Otrzymasz wsparcie w rozwiązaniu problemu, także w sprawach mieszkaniowych, zadłużeniach, świadczeń społecznych i innych.

Nieodpłatna Mediacja

Skorzystasz z pomocy mediatora, który pomoże Ci rozwiązać konflikt - bez konieczności kierowania sprawy do sądu.

KTO MOŻE SKORZYSTAĆ Z POMOCY?

- → każdy, kto nie jest w stanie ponieść kosztów odpłatnej pomocy prawnej
- → jednoosobowy przedsiębiorca, który w zeszłym roku nie zatrudniał żadnych pracowników
- → sygnaliści

! Wystarczy złożyć oświadczenie o braku możliwości poniesienia kosztów odpłatnej pomocy prawnej.

FORMA PORADY

Od stycznia 2026 r. **można wybrać formę porady** (**zdalna** lub **stacjonarna w punkcie**).

CZYM JEST PHISHING?

Phishing to najczęściej spotykana forma ataku socjotechnicznego wykorzystywana przez cyberprzestępców. Phishing to poważne zagrożenie dla bezpieczeństwa w sieci. Cyberprzestępcy wykorzystują coraz bardziej wyrafinowane metody, aby oszukać użytkowników i pozyskać ich poufne informacje. Aby się przed tym uchronić, warto przestrzegać podstawowych zasad bezpieczeństwa. W przypadku podejrzenia oszustwa, warto natychmiast podjąć odpowiednie kroki, aby zminimalizować jego skutki. Ochrona przed phishingiem działa na kilku poziomach i wymaga współpracy użytkowników, dostawców usług internetowych oraz firm specjalizujących się w bezpieczeństwie IT.

Phishing polega głównie na **podszywaniu się pod stronę internetową** w celu pozyskania danych logowania. Mogą to być na przykład dane logowania do konta e-mail, sieci komputerowej lub bankowości internetowej. To, co jest następnie robione z tymi danymi, różni się w zależności od sytuacji. Takie strony internetowe najczęściej przypominają witrynę organizacji/firmy/platformy/sklepu internetowego, pod które się podszywają. Cyberprzestępcy odtwarzają te witryny w taki sposób, że do złudzenia przypominają te oryginalne, które użytkownik zna i z których na co dzień korzysta, a adres URL strony phishingowej często przypomina również prawdziwy adres URL (najczęściej różni się od oryginału tylko jedną literą).

RODZAJE PHISHINGU

Spear phishing to odmiana phishingu, w której oszuści wymierzają atak na konkretne osoby lub organizacje. Cyberprzestępcy zbierają informacje na temat ofiary i jej zachowań w celu stworzenia bardziej wiarygodnej wiadomości e-mail;

Pharming to technika oszustwa, w której cyberprzestępcy przechwytują ruch

internetowy i przekierowują użytkowników na fałszywe strony internetowe, które wyglądają jak prawdziwe;

Clone phishing polega na stworzeniu fałszywej strony internetowej, która wygląda identycznie jak oryginalna. Cyberprzestępcy kopiują treści prawdziwej strony internetowej, aby przekonać użytkowników, że są na oryginalnej stronie;

Whaling cyberprzestępcy atakują wysoko postawione osoby w organizacji, aby zyskać w ten sposób zaufanie i nakłonić do udzielenia informacji, które nie powinny być dostępne osobom postronnym;

Smishing wykorzystuje wiadomości SMS zamiast wiadomości e-mail. Oszuści wysyłają fałszywe wiadomości tekstowe, w których proszą użytkowników o wprowadzenie swoich poufnych danych na fałszywej stronie internetowej;

Spoofing manipulacja adresem URL;

Social engineering przestępca konstruuje scenariusze, które mają na celu wyłudzenie cennych informacji.

JAK CYBERPRZESTĘPCY ZWABIAJĄ OFIARY?

E-mail to najczęstszy sposób zwabiania ofiar na stronę phishingową. Wiadomości phishingowe często wykorzystują pilną potrzebę, presję czasu i aktualne tematy. Na przykład przed Świętami Bożego Narodzenia podszywano się pod firmy kurierskie prosząc o dodatkowe dane do wysyłki przesyłki;

Ogłoszenia phisherzy mogą kupować reklamy w wyszukiwarkach takich jak Google czy Bing. Wiele osób klika najwyższy wynik wyszukiwania w wyszukiwarkach. Jeśli jest to reklama phishera, ktoś nieumyślnie ląduje na stronie phishingowej;

Social media kanały mediów społecznościowych są wykorzystywane do pozyskiwania danych osobowych;

Strony internetowe z produktami używanymi phisherzy mogą na przykład wysłać link za pośrednictwem stron sprzedaży internetowej (np. OLX) do fałszywej strony Blik lub banku, aby poprosić o płatność w wysokości 1 złotówki;

SMS („smishing") polega ona na wysyłaniu skróconego linku w wiadomości tekstowej. Otwarcie tego linku za pomocą smartfona powoduje przejście do strony phishingowej.

JAK DZIAŁA PHISHING?

Gdy cyberprzestępca uzyska dane użytkownika za pośrednictwem strony phishingowej, zostaną one wykorzystane do zalogowania się na prawdziwej stronie internetowej. W przypadku danych bankowych przestępca uzyska dostęp do konta bankowego. Obecnie firmy i organizacje dodają dodatkowe kroki uwierzytelniania, aby na przykład poprawić bezpieczeństwo kont bankowych. Cyberprzestępcy bardzo szybko ewoluują i wymyślają nowe sposoby na ominięcie lub zhakowanie tego uwierzytelnienia. Nie są to już strony, które proszą tylko o podanie nazwy użytkownika i hasła. W momencie, gdy użytkownik wprowadzi swoje dane na stronie phishingowej, **przestępca natychmiast loguje się do banku**, podczas gdy użytkownik nadal czeka na stronie phishingowej. Gdy przestępca zostanie poproszony o weryfikację, wysyła wiadomość za pośrednictwem strony phishingowej. W ten sposób użytkownik otrzymuje wiadomość, że musi zweryfikować swój login, np. za pomocą wiadomości tekstowej.

Za witryną phishingową kryje się **panel phishingowy**. Panel ten działa na infrastrukturze przestępców. Mogą oni hostować ten panel samodzielnie lub może to być zhakowana strona internetowa. W panelu przestępca widzi wszystkie zebrane dane. W momencie, gdy nowa osoba wprowadza swoje dane na stronie phishingowej, atakujący otrzymuje wyskakujące okienko z tymi samymi poufnymi informacjami.

Gotowy **zestaw phishingowy można kupić w dark necie** już za kilkadziesiąt dolarów. Dzięki temu przestępca nie musi być doświadczonym programistą, tak jak kiedyś. Przestępcy mogą samodzielnie zainstalować zestaw krok po kroku, zgodnie z instrukcją, po czym strona phishingowa jest natychmiast aktywna. Co więcej, aby manipulować płatnościami, przestępcy nie muszą nawet dobrze mówić po polsku.

Częstym celem phishingu są **klienci banków**. Dlatego instytucje te inwestują dużo pieniędzy i czasu w zapobieganie sytuacjom, w których ich klienci stają się ofiarami tej metody ataku. Dla wielu innych organizacji phishing jest mniej znanym zjawiskiem, ale stanowi realne zagrożenie.

JAK ROZPOZNAĆ PHISHING?

Próby phishingu można rozpoznać na kilka sposobów, które związane są z działaniami i charakterystycznymi cechami takich ataków. Przede wszystkim, warto zwrócić uwagę na:

- **niezwykłe lub nietypowe adresy email**, które mogą wydawać się podejrzane,
- ataki często wykorzystują **fałszywe strony logowania** odtwarzające wygląd popularnych witryn - różnice w detalu mogą zdradzić oszustwo,
- budzić niepokój powinno otrzymanie **prośby o podanie poufnych informacji** przez e-mail, sms, czy w rozmowie telefonicznej, takich jak dane logowania czy numery kart kredytowych,

- ataki phishingowe często przepełnione są **błędami ortograficznymi i gramatycznymi,**
- ponadto, wiadomości tego typu cechują się często **alarmującym tonem** - kreują pilną potrzebę działania, np. grożąc zablokowaniem konta.

METODY OCHRONY PRZED PHISHINGIEM

Istnieją efektywne metody obrony przed phishingiem, które obejmują zarówno technologiczne rozwiązania, jak i działania oparte na edukacji i świadomości użytkownika. Niezwykle ważne są **regularne aktualizacje systemów oraz zainstalowanych programów**, co znacznie utrudnia potencjalnym atakującym wykorzystanie znanych luk w oprogramowaniu. Instalowanie programu antywirusowego z wbudowanym filtrem anty-phishingowym to kolejny kluczowy krok w zabezpieczaniu systemu, ale najistotniejsza jest **edukacja użytkownika,** który powinien umieć odróżnić prawdziwe powiadomienia od prób phishingu. To oznacza, by zawsze sprawdzać adresy e-mail i webowe, unikać klikania w podejrzane linki oraz otwierania niezapowiedzianych załączników.

Pamiętaj, że nawet najbardziej zaawansowane technologie nie zastąpią zdrowego rozsądku i ostrożności.

W przypadku próby ataku phishingowego kluczowe jest zachowanie spokoju i podjęcie odpowiednich kroków. Po pierwsze, **nie należy odpowiadać na podejrzane maile, ani nie klikać w żadne zawarte w nich linki**. Następnie należy **zgłosić próbę ataku swojemu dostawcy usług internetowych** i poinformować swój bank, jeśli podejrzany e-mail zawierał dane do logowania do konta bankowego. Z ostrożności należy także **zmienić wszelkie hasła** do logowania do witryn, użytkowanych na danym urządzeniu (komputerze, laptopie czy telefonie).

PODSUMOWANIE

Phishing to poważne zagrożenie dla bezpieczeństwa w sieci. Cyberprzestępcy wykorzystują coraz bardziej wyrafinowane metody, aby oszukać użytkowników i pozyskać ich poufne informacje. Aby się przed tym uchronić, warto przestrzegać podstawowych zasad bezpieczeństwa. W przypadku podejrzenia oszustwa, warto natychmiast podjąć odpowiednie kroki, aby zminimalizować jego skutki. Ochrona przed phishingiem działa na kilku poziomach i wymaga współpracy użytkowników, dostawców usług internetowych oraz firm specjalizujących się w bezpieczeństwie IT.

ROZPOZNANIE PHISHINGU:

- Fałszywy adres e-mail lub strony internetowej;
- Błędy ortograficzne lub gramatyczne;
- Prośby o wprowadzenie poufnych informacji, takich jak hasła, numery kart kredytowych itp.;
- Prośby o natychmiastowe działanie;
- Dziwny wygląd lub układ strony internetowej.

ABY UNIKNĄĆ PHISHINGU:

Nie otwieraj wiadomości e-mail lub **nie klikaj w linki** pochodzące od nieznanych nadawców.
Nie wprowadzaj swoich poufnych informacji na nieznanych stronach internetowych.
Sprawdzaj dokładnie adres URL, a nie tylko obecność kłódki.
Używaj antywirusa i oprogramowania antyspamowego.
Regularnie aktualizuj oprogramowanie i **system operacyjny** swojego komputera i urządzeń mobilnych.

JEŚLI PADNIEMY OFIARĄ PHISHINGU, POWINNIŚMY NATYCHMIAST PODJĄĆ KILKA DZIAŁAŃ:

Wykonać skanowanie antywirusem i usunąć zainfekowane pliki lub zresetować swoje urządzenie do ustawień fabrycznych;
Zmienić hasła do wszystkich kont, na których używaliśmy tego samego hasła;
Skontaktować się z bankiem i powiadomić go o podejrzeniu oszustwa;
Zgłosić incydent na policji.

Nie ma sposobu, aby całkowicie powstrzymać phishing. Cyberprzestępcy będą zawsze próbowali oszukiwać użytkowników i pozyskiwać ich poufne informacje. Jednak poprzez stosowanie dobrych praktyk bezpieczeństwa i edukację na temat phishingu, możemy zmniejszyć ryzyko wpadnięcia w pułapki oszustów.

OCHRONA PRZED PHISHINGIEM DZIAŁA NA KILKU POZIOMACH:

- **Edukacja użytkowników** na temat phishingu i dobrych praktyk bezpieczeństwa;
- Używanie **oprogramowania antywirusowego**, antyspamowego do blokowania podejrzanych wiadomości e-mail i SMS;
- **Analiza zachowania użytkownika** w celu wykrycia podejrzanych aktywności, takich jak próby logowania na nieznane urządzenia czy wprowadzanie nieprawidłowych haseł;
- **Automatyczne blokowanie podejrzanych stron internetowych** i wiadomości e-mail przez systemy bezpieczeństwa;
- **Wdrażanie procedur reagowania na incydenty**, które pozwalają szybko zareagować na ataki phishingowe i minimalizować ich skutki.

Informator zawiera stan prawny na: czerwiec 2026 r.

Miejsce na notatki:

Ponad połowa punktów nieodpłatnej pomocy prawnej i nieodpłatnego poradnictwa obywatelskiego w Polsce jest prowadzona przez organizacje pozarządowe, jako zadanie publiczne powierzane przez starostów lub prezydentów, w efekcie corocznego, otwartego konkursu ofert.

SURSUM CORDA oznacza „w górę serca!”.
W tym zawołaniu zawiera się cała nasza misja – pomagać w trudnej sytuacji i dawać nadzieję na to, że może być lepiej. Dla tych, którzy chcą się angażować i wspierać projekty dobroczynne - tworzymy warunki do skutecznego działania, w klimacie zaufania i czytelnych zasad.

Jedną z form naszej aktywności jest prowadzenie od 2016r. sieci punktów nieodpłatnej pomocy prawnej, poradnictwa obywatelskiego i mediacji oraz urozmaicona edukacja prawna.

Stowarzyszenie Sursum Corda powstało w 2000 r. z inicjatywy grupy przyjaciół i profesjonalistów, którzy wcześniej – przez 6 lat – angażowali się społecznie jako wolontariusze. Jako organizacja pozarządowa **jesteśmy apolityczni działamy na zasadzie „non profit”, czyli nie dla zysku.**

Posiadamy status organizacji pożytku publicznego, co oznacza, że możesz przekazać nam 1,5% podatku, który codziennie inwestujemy w mądre pomaganie.

Będzie nam miło, jeśli dołączysz do naszej załogi!

sursum corda
STOWARZYSZENIE w górę serca

wolontariat na ratunek

NIEODPŁATNE USŁUGI
-POMOC PRAWNA
-PORADY OBYWATELSKIE
-MEDIACJA

wypoczynek na plus

POMOC seniorom

wypożyczalnia
SPRZĘTU REHABILITACYJNEGO I MEDYCZNEGO

szkolenia

POMOC ukrainie

1,5% pomoc ma moc!

KRS 00000 20382

Rozlicz swój PIT za darmo!

www.sc.org.pl