

Warszawa, 16 października 2019 r.

IOD-042-134/2019



Jak postępować w przypadku fałszywych wiadomości e-mail?

Phishing

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych do logowania, szczegółów dot. tożsamości osoby, której dane dotyczą) albo nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej¹.

Na czym polega wyłudzenie informacji?

Wyłudzenie informacji zwykle odbywa się za pośrednictwem e-maili, reklam lub stron, które wyglądają podobnie do stron, z których korzystamy. Przestępca próbując wyłudzić informacje, może wysłać maila, który wygląda, jakby został wysłany przez określoną instytucję np. Uniwersytet Warszawski i zawiera prośbę o podanie: danych do logowania, numeru PESEL, kodu PIN do karty płatniczej, daty urodzenia lub nakłania do otworzenia zainfekowanego załącznika czy kliknięcia we wskazany w wiadomości link.

Jak rozpoznać fałszywą wiadomość e-mail?



- zawsze sprawdzaj adres nadawcy i uważaj na dziwne adresy. Poprawny adres mailowy powinien zawierać nazwę domeny, np.: adm.uw.edu.pl, uw.edu.pl²,
- sprawdź nagłówki wiadomości, aby upewnić się, że nagłówek „Od” („From”) zawiera właściwy adres nadawcy;



- **nie należy działać pochopnie**, fałszywa wiadomość e-mail często informuje użytkownika o tym, że: bezpieczeństwo jego konta jest zagrożone,

¹ <https://pl.wikipedia.org/wiki/Phishing>, dostęp: 16.10.2019 r.

² Domena Uczelniana nie zawsze gwarantuje, że wiadomość została wysłana z Uczelni. W Internecie funkcjonują strony internetowe pozwalające użyć np. ogólnodostępnego adresu mailowego i ukryć tożsamość faktycznego nadawcy wiadomości.

przekroczono ilość miejsca przeznaczoną na przechowywanie wiadomości, konto wymaga działania administratora poczty;



- zachowaj czujność, jeżeli wiadomość e-mail rozpoczyna się np. słowami: Pozdrowienia z Uniwersytetu Warszawskiego, Jesteśmy Uniwersytetem Warszawskim pod kierownictwem, Drogi Użytkowniku, Drogi, Droga [adres e-mail];



- błędy w pisowni lub błędy gramatyczne powinny wzbudzić podejrzenia,
- ostrożnie podchodź do gróźb i pilnych terminów;



- nie otwieraj załączników i nie klikaj w link, jeżeli nie masz 100% pewności, że wiadomość pochodzi z wiarygodnego źródła.

Jak zadbać o swoje bezpieczeństwo?

- **zachowaj rozsądek** – ryzyko zostania ofiarą oszustów będzie mniejsze, gdy zachowasz się rozsądnie podczas przeglądania stron internetowych i wiadomości e-mail,
- nawet jeśli domena adresu mailowego lub link do strony wskazuje, że wiadomość została wysłana z Uniwersytetu Warszawskiego, **nie oznacza to, że jest to wiadomość autentyczna**,
- adresy URL zawierające domenę Uniwersytetu Warszawskiego **nie zawsze muszą być prawdziwe**,
- adresy URL w domenie UW, zazwyczaj są zaszyfrowane za pomocą szyfrowania SSL – link zaczyna się od **https://** - s wskazuje, że połączenie ze stroną jest zabezpieczone szyfrowaniem*,
- zwracaj uwagę na symbol zamkniętej kłódki widoczny w pasku adresu – oznacza to, że połączenie ze stroną jest bezpieczne*,
- jeżeli podejrzewasz, że padłeś ofiarą phishingu lub w inny sposób uzyskano Twoje dane – **natychmiastowo zmień hasło** oraz pytania zabezpieczające,
- jeżeli możesz skorzystać z uwierzytelniania dwuskładnikowego – **stosuj takie rozwiązanie**,
- jeżeli uważasz, że doszło do naruszenia **powstrzymaj się od dalszego działania na urządzeniu**,
- zgłoś podejrzenie naruszenia/incydentu bezpieczeństwa informacji i danych osobowych – informatykowi, Inspektorowi Ochrony Danych, bezpośrednio przełożonemu – **działaj szybko**,
- korzystaj z programów antywirusowych,
- aktualizuj oprogramowanie,
- ograniczaj możliwość wglądu w zawartość ekranu urządzenia z którego korzystasz,
- zachowaj hasła tylko dla swojej wiadomości,
- nie stosuj tych samych haseł do kont prywatnych i służbowych,
- nie korzystaj z niezabezpieczonych sieci Wi-Fi w kawiarniach, restauracjach innych miejscach publicznych,

* Należy pamiętać, iż przestępca ma tego świadomość i może przygotować spreparowaną witrynę zgodnie z dobrymi praktykami w zakresie zabezpieczeń. Więcej o https i „kłódce” można przeczytać tutaj: <https://plblog.kaspersky.com/https-does-not-mean-safe/8789/>, dostęp: 16.10.2019 r.

- szyfruj dyski stacji roboczych i laptopów, a także zewnętrzne nośniki danych jak płyty CD, DVD oraz pamięci flash (pendrive).

Jak sprawdzić czy dam się nabrać na phishing?

- przetestuj się korzystając z quizu Google:
<https://phishingquiz.withgoogle.com/>

Jak sprawdzić czy mój adres e-mail nie był przedmiotem wycieku danych („nie został skompromitowany”)?

- portale społecznościowe, sklepy internetowe, aplikacje webowe, przechowują nasze dane prywatne – imiona i nazwiska, adresy zamieszkania, zdjęcia, numery kont bankowych i wiele innych – pamiętaj, że do Twoich danych dostęp mogą uzyskać osoby nieuprawnione,
- aby sprawdzić czy Twój adres e-mail był przedmiotem wycieku danych skorzystaj ze stron:
<https://haveibeenpwned.com/>
<https://monitor.firefox.com/>


Przykładowe maile phishingowe

Zapytanie o wycenę (UNIwersYTET WARSZAWSKI) UNI784/WA987.

Uniwersytet Warszawski <admin@uw.edu.pl> 10.10.2019 09:32 UW

Do undisclosed-recipients,
Odpowiedz Odpowiedz wszystkim Prześlij dalej Usuń

3 załączniki Widok Pobierz




Pozdrowienia,

Zgodnie z dobrymi zaleceniami Twojej firmy jesteśmy polską uczelnią pod kierunkiem dr Marcina Pałysa. Potrzebujemy Twojej oferty cenowej do naszego budżetu na 2019 r. (W załączeniu)
Prześlij swoją ofertę z wyprzedzeniem, termin składania ofert upływa 18 października 2019 r.

miłego dnia

UNIwersYTET WARSZAWSKI



Dr. Marcina Pałysa

Krakowskie Przedmieście 28/28
00-927 Warszawa
tel. +48 22 55 20 011
NIP 525-001-12-88
admin@uw.edu.pl

Przykładowe maile phishingowe

--- Treść przekazanej wiadomości ---

Temat: Uniwersytet Warszawski Żądanie oferty cenowej

Data: Wed, 09 Jan 2019 00:47:10 +1300

Nadawca: Professor Marcin Pałys <rektor1@adm.uw.edu.pl>

Odpowiedź-Do: Uniwersytet Warszawski <visual4life@outlook.com>

Adresat: Dostawca <vendor1829@adm.uw.edu.pl>



Powyższa instytucja polska uprzejmie prosi wszystkie rodzime firmy z Polski, aby zacytowały nas w załączonym zapytaniu ofertowym dla naszych proponowanych projektów

Data zamknięcia jest 20 stycznia 2019 roku

Oczekiwanie na najszybsze notowania najniższej ceny

pozdrawiam

Professor Marcin Pałys



ph.: (+48) 22 55 20 355,

(+48) 22 55 20 342

fax: (+48) 22 55 24 000

e-mail: rektor@adm.uw.edu.pl

Przykładowe maile phishingowe

WNIOSEK O OFERTĘ (Uniwersytet Warszawski) EUI894/BU4600 - Wiadomość

Plik Wiadomość ESET Acrobat Powiedz mi, co chcesz zrobić...

Ignoruj Wiadomości-śmieci Usun Odpowiedz Odpowiedz wszystkim Prześlij dalej Więcej Przenieś Reguły OneNote Akcje Oznacz jako nieprzeczytane Kategorie Znaczniki Przetłumacz Znajdź Pokrewne Zaznacz Powiększ

Usuwanie Odpowiadanie Przenoszenie Znaczniki Edytowanie Powiększenie

sr. 07.08.2019 09:14




Uniwersytet Warszawski <iod@adm.uw.edu.pl>

WNIOSEK O OFERTĘ (Uniwersytet Warszawski) EUI894/BU4600

Do undisclosed-recipients:

i Ta wiadomość została wysłana z ważnością: Wysoki.
W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.
Kliknij tutaj, aby pobrać obrazy. Aby pomóc ochronić prywatność, program Outlook uniemożliwił automatyczne pobranie niektórych obrazów znajdujących się w tej wiadomości.

Załącznik bez tytułu 00...
0 B

Pozdrowienia z Uniwersytetu Warszawskiego,

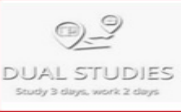

Załącz:

Zgodnie z dobrymi rekomendacjami Twojej firmy jesteśmy Uniwersytetem Warszawskim pod kierunkiem prof. Marcina Pałysa.

Potrzebujemy Twojej oferty cenowej dla naszego budżetu 2019 (w załączeniu).

Prosimy o przesłanie oferty w terminie do 9 sierpnia 2019 r.

Pozdrowienia.

Uniwersytet Warszawski
ul. Krakowskie Przedmieście 26/28
00-927 Warszawa

tel.: +48 22 55 20 000, fax: +48 22 55 24 029
NIP 525-001-12-66
REGON 000001258

E-mail:

