UNIWERSYTET WARSZAWSKI
Inspektor Ochrony Danych

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 społecznej[1].

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.pl[2],
- 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 wysyłana 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 http**s**:// - 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, bezpośredniemu 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?

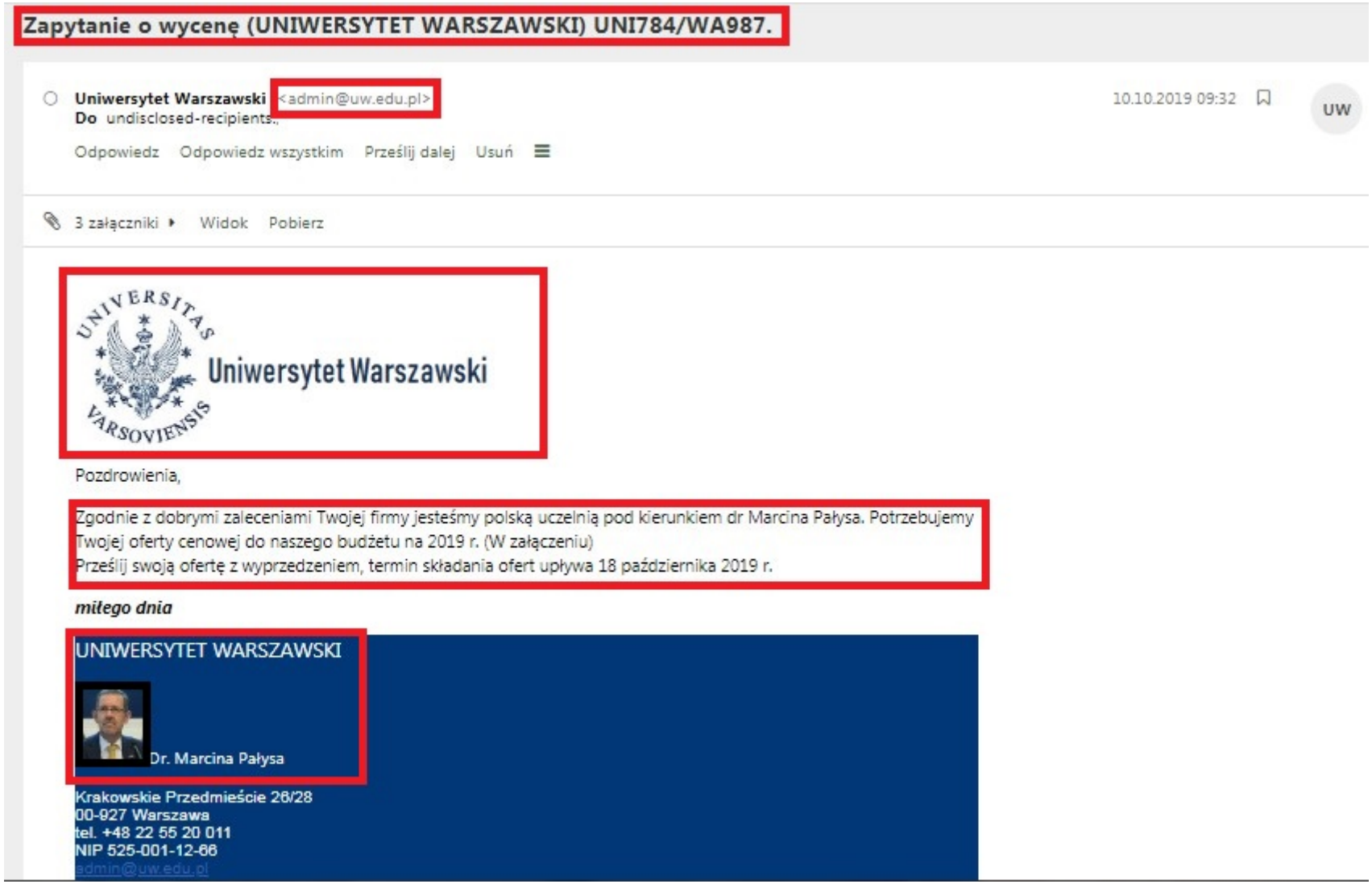
- przetestuj się korzystając z quizu Google:
  https://phishingquiz.withgoogle.com/

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



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>

Szanowni Państwo

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

pozdrowienia

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