**UWAGA: Phishing**

**Phishing** – to metoda oszustwa, w której przestępca podszywa się pod inną osobę
lub instytucję w celu:

* wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej),
* zainfekowania komputera szkodliwym oprogramowaniem
* nakłonienia ofiary do określonych działań.

Jest to bardzo prosty rodzaj ataku cybernetycznego, opartego na inżynierii społecznej, czyli stosowaniu socjotechnicznych metod manipulacji i środków psychologicznych mających na celu wywołanie pożądanych reakcji odbiorcy. Phishing nie wymaga posiadania zaawansowanej wiedzy technicznej ani szukania luk w zabezpieczeniach, ponieważ bazuje na najsłabszym ogniwie ochrony sieci komputerowej, czyli błędach użytkownika. Twórcy fałszywych informacji podszywają się pod realnie istniejące instytucje, nakłaniając użytkownika do określonych zachowań.

Oszuści wykorzystują ciekawość, poczucie obowiązku, chęć korzystania z prawidłowo funkcjonujących narzędzi pracy (ale również podatność na stres wywołany tzw. presją czasu, roztargnienie, łatwe uleganie wpływom) oraz stosują metody mające wzbudzić strach i wymusić pośpiech w działaniu.

**Przykład phishingu:**

*(jest to wiadomość rzeczywiście otrzymana przez Inspektora Ochrony Danych UEK)*

**Od:** "Zimbra1) WorldClient" <noreply@administration.com>
**Do:** iod@uek.krakow.pl
**Wysłane:** wtorek, 9 listopada, 2021 8:27:50
**Temat:** Admin2) Support3)

Drogi iod@uek.krakow.pl,

Twoje konto nie przeszło procesu weryfikacji/aktualizacji4). Oczekuje się, że właściciele kont zaktualizują swoje konta. Niezastosowanie się do tego powiadomienia
w określonym czasie może uniemożliwić wysyłanie lub odbieranie wszystkich wiadomości, a właściciel będzie narażony na ryzyko utraty swojego konta.
[Kliknij](https://thegrapetaste.net/Web-Client-Upgrade/)5), aby zaktualizować swoje konto.

UWAGA!!! Jeśli nie zaktualizujesz swojego konta, Twoje konto zostanie automatycznie usunięte z naszego systemu6).

Przepraszamy za wszelkie związane z tym niedogodności.

Z poważaniem
Obsługa klienta7)
Zespół wsparcia technicznego8)

           Copyright © 2005-2021 Synacor, Inc. Wszelkie prawa zastrzeżone9)

**Na co należy zwracać uwagę:**

* 1) aby się uwiarygodnić, fałszywy nadawca często używa nazwy, która jest znana albo kojarzona przez odbiorcę (tutaj: Zimbra, którą wszyscy znamy, jako system naszej poczty elektronicznej)
* 2) i 3) fałszywy nadawca często posługuje się określeniami o znaczeniu technicznym
lub informatycznym (tutaj: Admin oznacza administratora sieci/systemu, Support oznacza wsparcie, pomoc)
* 4) fałszywy nadawca często odwołuje się do określeń wskazujących, że coś jest sprawdzane i nie działa prawidłowo, z jednoczesnym przekazem, że winny jest odbiorca wiadomości (tutaj: **Twoje** konto **nie przeszło** procesu weryfikacji/aktualizacji)
* 5) fałszywy nadawca często stosuje metody nacisku lub nakazu, w celu wywołania pożądanej reakcji (tutaj: **Kliknij**) i od razu „podpina” link, który przekierowuje na nieznaną stronę
* 6) fałszywy nadawca często stosuje metody groźby oraz przedstawia perspektywę
jej natychmiastowego zrealizowania w przypadku niezastosowania się odbiorcy do nakazu (tutaj: **jeśli nie** zaktualizujesz, konto zostanie **automatycznie** usunięte)
* 7) i 8) aby się uwiarygodnić, fałszywy nadawca często podpisuje się jako podmiot, który dba i troszczy się o dobro odbiorcy wiadomości (tutaj: **Obsługa** klienta, zespół **wsparcia** technicznego)
* 9) fałszywy nadawca często używa symboli i znaków graficznych, które odbiorca wiadomości kojarzy z ochroną prawną, co dodatkowo ma wzbudzić jego zaufanie
(tutaj: Copyright oznacza ochronę praw autorskich, Synacor to nazwa firmy będącej dostawcą usług poczty e-mail).

**Jeśli otrzymana wiadomość z jakichkolwiek powodów wydaje Ci się podejrzana
- aby nie stać się ofiarą phishingu i nie narażać siebie i pracodawcy na ryzyko naruszenia ochrony danych – pamiętaj:**

1. Nie spiesz się z reakcją
2. Nie klikaj w podane linki
3. Nie otwieraj załączników
4. Przekaż maila na adres: kepperta@uek.krakow.pl w celu jego dokładnego sprawdzenia
i ewentualnego zablokowania nadawcy.