# Warto wiedzieć…

## Phishing – czyli jak nie dać się złowić w sieci

Phishing – to oszustwo polegające na wyłudzaniu danych osobowych przez podawanie się za kogoś innego. Oszuści najczęściej próbują zdobyć dane lub pieniądze, podszywając się pod instytucje obdarzane przez nas zaufaniem np. pocztę, firmy dostarczające energię lub wodę, banki, organy ścigania itp. Eksperci wyróżniają takie rodzaje phishingu jak smishing (przy użyciu SMS'ów), vishing (przez telefon) oraz spear-phishing (wymierzony w konkretną osobę).

Istnieje kilka zasad, które pomogą Ci ustrzec się przed atakiem phishingowym:

1. Ogranicz do minimum ilość informacji o sobie i bliskich Ci osobach, które udostępniasz w sieci.
2. Bądź uważny. Oszuści mogą tworzyć wierne kopie stron, które odwiedzasz. Dlatego zwracaj szczególną uwagę na to czy adres WWW jest poprawny.
3. Jeśli tylko jest taka możliwość, zawsze używaj uwierzytelniania dwuskładnikowego i silnych haseł.
4. Śledź informacje w mediach o wyciekach danych.
5. Korzystaj tylko z renomowanych platform i stron. Szczególnie uważaj przy robieniu zakupów w sieci. Jeśli jakaś oferta wydaje się być zbyt dobra by była prawdziwa – bardzo prawdopodobne, że masz do czynienia z oszustwem.
6. Zachowaj spokój, nie ulegaj presji, nie podejmuj decyzji dotyczących Twoich danych w pośpiechu. Oszuści mogą próbować wywrzeć presję albo wywołać Twój niepokój. Najlepiej skonsultuj się z rodzicem lub inną osobą dorosłą zanim przekażesz jakiekolwiek dane przez telefon albo e-mail.
7. Używaj kliku adresów e-mail. Jeśli stracisz dostęp do jednej skrzynki w wyniku ataku phishingowego, będzie to mniejsza strata, gdy używasz kilku adresów e-mail do obsługi swoich spraw w sieci np. szkolnych, gier lub innych subskrypcji.
8. W poczcie e-mail używaj filtra antyspamowego w celu zminimalizowania ilości otrzymywanego spamu, a co za tym idzie zmniejszenie szansy na oszustwo phishingowe.

Jeśli jednak dasz się złowić w sieci koniecznie powiedz o tym rodzicom. W następnej kolejności warto poinformować bank, policję lub instytucję bądź firmę, pod którą podszywali się oszuści. Wypełnij też formularz zgłoszenia incydentu na stronie CERT Polska - https://incydent.cert.pl/
Koniecznie zmień również swoje dane logowania.

URZĄD OCHRONY DANYCH OSOBOWYCH

# Fiszki

Phishing – określenie wywodzące się z angielskiego słowa *fishing* oznaczającego łowienie, wędkowanie. Phishing to wszelkie próby wyłudzenia danych osobowych przez oszustów podszywających się pod godne zaufania podmioty.

Spear-phising – spersonalizowana forma phishingu, której celem jest wyłudzenie danych konkretnej osoby przy użyciu np. bezpośredniej korespondencji przez e-mail, SMS lub przez rozmowę telefoniczną.

Vishing – forma phishingu polegająca na wyłudzeniach danych w trakcie bezpośredniej rozmowy telefonicznej

Smishing – popularny wśród oszustów sposób ataku skierowany na dane osobowe przy użyciu wiadomości SMS, które najczęściej zawierają podejrzane linki lub oferty.

Uwierzytelnianie dwuskładnikowe – sposób na dodatkowe potwierdzenie tożsamości osoby, która loguje się na swoje konto. Oprócz zwykłego hasła, w przypadku uwierzytelniania dwuskładnikowego logujący się, musi podać najczęściej kod otrzymany na telefon lub z tokena.

Silne hasło – jest trudne do odgadnięcia i zawiera co najmniej 8 znaków, w tym litery (małe i wielkie), cyfry i znaki specjalne jak #,!?>. Silne hasło nie powinno być również słowem, które można znaleźć w słowniku, ani imieniem, lub nazwiskiem bliskiej osoby. Do każdego konta powinieneś używać innego hasła.