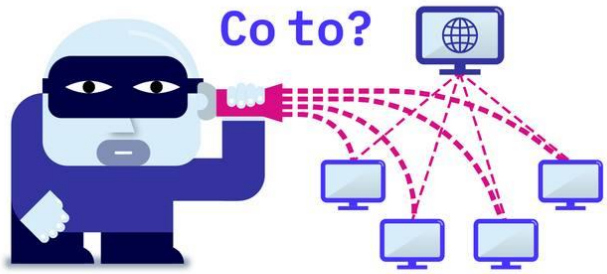
//: PHISHING VISHING SPOOFING </>

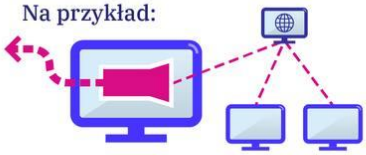
>0< SNIFFING ?!..

Co to?



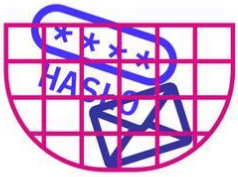
Technika wykorzystywana przez cyberprzestępców w celu **pozyskiwania poufnych informacji**. Polega na przechwytywaniu pakietów danych **przekazywanych przez sieć** („podsłuchanie" przez sieć).

Na przykład:



zainstalowanie na komputerze sniffera, czyli programu służącego „podsłuchiwaniu" ruchu sieciowego

Czym grozi?



przejęciem przez przestępców wiadomości mailowych, haseł

Jak się chronić?

unikaj używania publicznego i niezabezpieczonego Wi-Fi

nie klikaj w podejrzane linki

korzystaj wyłącznie z bezpiecznych i szyfrowanych komunikatorów i skrzynek pocztowych

korzystaj z programów antywirusowych

Wiemy! BEZPIECZNI W BANKU I W NECIE

Infografika przygotowana przez: INPRIS

Projekt finansowany przez: Santander Fundacja

//: VISHING SNIFFING SPOOFING </>

>0< PHISHING ?!..

Co to?

Oszustwo polegające na tym, że **przestępca podszywa się** pod inną osobę / instytucję w celu **wyłudzenia danych** lub nakłonienia adresata do określonych działań.

Na przykład:

SMS z „banku" z prośbą o podanie hasła

e-mail z linkiem do fałszywej strony logowania

e-mail z prośbą o zapłatę faktury z podmienionym numerem konta

Czym grozi?

ujawnieniem poufnych informacji (np. haseł, danych karty płatniczej)

zainfekowaniem komputera / telefonu szkodliwym oprogramowaniem

nakłonieniem ofiary do określonych działań (np. przelewu na nieznany numer konta)

Jak się chronić?

nigdy nie podawaj poufnych danych (login, hasło, numer karty) w odpowiedzi na e-maile / SMS-y lub przez umieszczone tam formularze

nie klikaj w linki zawarte bezpośrednio w treści e-maila/SMS-a

przy logowaniu do banku weryfikuj, czy adres strony www zaczyna się od liter **https** (bezpieczny protokół)

w razie wątpliwości skontaktuj się z nadawcą, żeby potwierdzić autentyczność wiadomości

Wiemy! BEZPIECZNI W BANKU I W NECIE

Infografika przygotowana przez: INPRIS

Projekt finansowany przez: Santander Fundacja

//: PHISHING VISHING SNIFFING </>

>0< SPOOFING ?!..

Co to?

Oszustwo polegające na tym, że **przestępca (haker) podszywa się pod** inne urządzenie lub użytkownika sieci, żeby **wykraść poufne dane** lub zainstalować **złośliwe oprogramowanie**.

Na przykład:

oszukanie sieci w celu skierowania użytkownika na podrobione strony www

podrobienie nagłówka e-mail tak, aby wyglądał jak od konkretnej osoby

Czym grozi?

ujawnieniem poufnych informacji (np. haseł, danych karty płatniczej)

zainfekowaniem komputera / telefonu szkodliwym oprogramowaniem

Jak się chronić?

nigdy nie podawaj poufnych danych (login, hasło, numer karty) **w odpowiedzi na e-maile / SMS-y**

sprawdzaj dokładnie, czy adres mailowy nadawcy nie jest podejrzany (nie tylko nazwę nadawcy)

zwracaj uwagę, czy strona internetowa / przeglądarka nie zachowują się dziwnie lub inaczej niż zwykle

korzystaj z programów anty-wirusowych

Wiemy! BEZPIECZNI W BANKU I W NECIE

Infografika przygotowana przez: INPRIS
Projekt finansowany przez: Santander Fundacja

//: PHISHING SPOOFING SNIFFING </>

>0< VISHING ?!..

Co to?

Oszustwo polegające na tym, że przestępca **podszywa się** pod inną osobę / instytucję, żeby **wyłudzić poufne dane** za pośrednictwem **rozmowy telefonicznej**.

Na przykład:

telefon z „banku" z prośbą o podanie loginu

telefon od „ubezpieczyciela" z prośbą o podanie numeru PESEL

Czym grozi?

ujawnieniem poufnych informacji (np. haseł, danych karty płatniczej, numeru PESEL)

Jak się chronić?

nigdy nie podawaj przez telefon danych poufnych jak login, hasło, numer karty, kod PIN, kod CVV

zawsze sprawdzaj osobę, z którą rozmawiasz np. prosząc o telefon za chwilę w celu zweryfikowania tożsamości dzwoniącego przez stronę internetową banku lub oficjalną infolinię

w razie próby manipulacji / wyciągnięcia informacji przerwij połączenie i zablokuj numer

Wiemy! BEZPIECZNI W BANKU I W NECIE

Infografika przygotowana przez: INPRIS
Projekt finansowany przez: Santander Fundacja