wrocławskie
centrum rozwoju
społecznego

Szanowni Państwo,

W związku z powziętymi informacjami od radnych osiedlowych dotyczących ataków phishingowych za pośrednictwem skrzynek e-mailowych rad osiedla, prosimy o wzmożoną czujność i ostrożność, w szczególności na fałszywe załączniki i próby wyłudzenia danych logowania do poczty osiedlowej! Na Państwa skrzynkę pocztową mogą trafiać wiadomości pochodzące od przestępców, zawierające złośliwe załączniki lub odnośniki kierujące do nieprawdziwych stron łudząco przypominających pocztę osiedlową, za pośrednictwem których mogą zostać wykradzione Państwa dane logowania.

Prosimy o zastosowanie poniższych zasad bezpieczeństwa:

1. Zanim klikną Państwo w link proszę o upewnienie się, że otrzymana wiadomość pochodzi z adresu kończącego się na @wcrs.pl.
2. Prosimy o niepodawanie swoich danych do logowania na stronach, do których kieruje link z podejrzanej wiadomości.

Phishing jest najprostszym, a jednocześnie najskuteczniejszym i najpopularniejszym rodzajem ataku, na który narażeni są praktycznie wszyscy.

Phishing to rodzaj oszustwa polegającego na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia informacji, zainfekowania sprzętu złośliwym oprogramowaniem lub nakłonienia ofiary do określonych działań.

Do ataków typu phishing wykorzystywane są wszystkie formy komunikacji elektronicznej:
- wiadomości e-mail
- SMS-y
- wiadomości na komunikatorach (np. WhatsApp)
- wiadomości prywatne w serwisach społecznościowych (np. na Instagramie)
- rozmowy telefoniczne

Phishing – w przeciwieństwie do innych ataków komputerowych, które wykorzystują błędy, luki czy słabości w oprogramowaniu i jego konfiguracji – skupia się na wykorzystaniu metod takich jak socjotechnika lub inżynieria społeczna. Celem ataku phishingowego nie jest sprzęt czy oprogramowanie, ale sam człowiek.

W przypadku phishingu atakujący korzysta najczęściej z autorytetu osoby lub instytucji, pod którą się podszywa, kontaktując się np. jako przełożony, pracownik z urzędu, kolega z pracy, bank, dostawca prądu, urząd, firma przewozowa lub znany sklep.

Treść wiadomości najczęściej ma za zadanie wzbudzić w odbiorcy silne emocje takie jak strach czy wymusić pośpiech, aby skłonić ofiarę do szybkiego działania, którego oczekuje atakujący.

Działaniami, do których ma skłaniać wiadomość phishingowa są często na przykład:
- podanie danych logowania do banku na spreparowanej stronie WWW
- podanie danych karty płatniczej / kredytowej
- wpisanie loginu i hasła logowania do skrzynki pocztowej czy innego serwisu internetowego po kliknięciu w link z wiadomości
- podanie danych osobowych (np. PESEL, nazwisko panieńskie matki, data urodzenia, miejsce urodzenia, numer dowodu) potrzebnych do uzyskania dostępu do niektórych kont lub np. zaciągnięcia kredytu
- pobranie pliku ze złośliwym oprogramowaniem (np. faktury, wezwania do zapłaty, pisma od kancelarii prawnej)
- instalacja złośliwego oprogramowania (np. ransomware, trojana, wirusa).

pl. Dominikański 6
50-159 Wrocław
telefon: 71 77 24 900
faks: 71 77 24 939
e-mail:
info@wcrs.wroclaw.pl
NIP:
8971748403
REGON:
020880445

wrocławskie
centrum rozwoju
społecznego

W lipcu 2024 roku otrzymaliśmy zgłoszenie, że doszło do serii ataków phishinowych na Państwa skrzynki osiedlowe. Atakujący mogli uzyskać dostęp do danych osobowych zawartych w wiadomościach e-mail, w tym imion, nazwisk oraz adresów e-mail mieszkańców. W wyniku tego naruszenia istnieje ryzyko, że dane osobowe mogły zostać wykorzystane przez nieuprawnione osoby, co może prowadzić do otrzymywania niechcianych wiadomości (spam) lub potencjalnie innych działań, jak próby wyłudzeń. W odpowiedzi na to zdarzenie natychmiast podjęliśmy kroki mające na celu zabezpieczenie naszych systemów.

Zablokowaliśmy adresy, z których były przeprowadzane ataki oraz zmieniliśmy hasła do wszystkich potencjalnie zaatakowanych skrzynek e-mail. Dodatkowo rozesłaliśmy również informacje na skrzynki osiedlowe z prośbą o regularną zmianę haseł i zachowanie szczególnej ostrożności w komunikacji e-mailowej.

Jeśli mają Państwo jakiekolwiek pytania lub wątpliwości, prosimy o kontakt z naszym Inspektorem Ochrony Danych, pod adresem e-mail: iod@wcrs.pl