Realizując zadania wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 ze zm.) przedstawiamy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa, zagrożeń i sposobów zabezpieczenia się przed nimi.

Przykłady różnych form wyłudzeń, na które użytkownik internetu może być narażony:

Phishing: Jest to jedna z najpopularniejszych form wyłudzeń online. Atakujący wysyłają wiadomości e-mail, które wyglądają, jakby pochodziły od zaufanej strony (na przykład od banku lub serwisu społecznościowego). Te wiadomości zazwyczaj zawierają linki prowadzące do fałszywych stron internetowych, które wyglądają jak prawdziwe, a które próbują skłonić ofiary do podania swoich danych logowania, numerów kart kredytowych lub innych informacji.

Scam (Oszustwa): Oszustwa online mogą przyjmować różne formy. Przykładowo, oszustwo „Nigerijski Princ" polega na tym, że osoba otrzymuje wiadomość od kogoś, kto twierdzi, że jest księciem lub odziedziczył spadek i potrzebuje pomocy finansowej w zamian za dużą sumę pieniędzy w przyszłości. Inne typowe oszustwa to te związane z loteriami, pracą, romansami czy inwestycjami.

Ransomware: Jest to typ złośliwego oprogramowania, który po zainstalowaniu na komputerze blokuje dostęp do danych lub całego systemu, a następnie żąda od ofiary okupu (zazwyczaj w kryptowalutach) za odblokowanie.

Man-in-the-Middle Attack: Atakujący próbuje przechwycić komunikację między dwiema stronami w celu wykradzenia informacji, takich jak dane do logowania lub informacje o karcie kredytowej.

Spoofing: Polega to na podszywaniu się pod inny adres IP lub adres e-mail w celu oszustwa, rozmowy lub zdobycia nieautoryzowanego dostępu do systemu.

Fałszywe sklepy internetowe: Fałszywe sklepy internetowe to strony, które wyglądają jak prawdziwe sklepy online, ale które są stworzone tylko po to, aby wykradać dane karty kredytowej lub innego rodzaju płatności od kupujących. Często przyjmują opłatę za przedmiot wystawiony na sprzedaż w sklepie natomiast nigdy go nie wysyłają. Potrafią budować też reputację przez wysyłkę kilku przedmiotów zgodnych z opisem w sklepie celem uzyskania pozytywnych opinii i komentarzy.

Preteksting: Ten rodzaj ataku polega na tworzeniu przekonujących scenariuszy i kontekstów, które skłaniają ofiarę do podania swoich danych osobowych. Na przykład, atakujący może twierdzić, że dzwoni z banku i potrzebuje potwierdzenia pewnych informacji.

Wiadomości o wygranej nagrodzie: Oszustwo polegające na informowaniu ofiary, że wygrała nagrodę (taką jak loterię, konkurs czy darmowe produkty), ale musi najpierw zapłacić „opłatę administracyjną" lub podać dane osobowe i finansowe.

Wiadomości od „znajomego w potrzebie": Oszustwo polegające na wysłaniu wiadomości, która wydaje się pochodzić od znajomego lub członka rodziny potrzebującego pilnej pomocy finansowej. Zwykle oszust twierdzi, że jest zagranicą lub uległ wypadkowi i nie ma dostępu

do swoich kont. Wiadomości często przesyłane są z kont społecznościowych przejętych przez oszusta.

Fałszywe aukcje online: W tym przypadku oszust wystawia na aukcję przedmiot, którego nie posiada lub który nie istnieje, a po otrzymaniu zapłaty, nie wysyła przedmiotu. Drugim sposobem oszusta jest wystawienie przez niego na sprzedaż przedmiotu mającego atrakcyjną cenę i informowanie potencjalnych klientów i nieodzownym wpłaceniu zaliczki celem wykonania rezerwacji przedmiotu sprzedaży.

Fałszywe ogłoszenia o pracę: Oszuści publikują fałszywe oferty pracy, często oferując atrakcyjne warunki, takie jak praca z domu. Po otrzymaniu aplikacji, oszuści oczekują CV, które służą do kradzieży tożsamości lub mogą próbować oszukać kandydatów na inne sposoby, na przykład żądając opłaty za „szkolenie" lub „materiały".

Oszustwa związane z kryptowalutami: Ataki te mogą obejmować fałszywe platformy inwestycyjne, phishing kryptowalutowych portfeli czy schematy typu „pump and dump", gdzie oszuści sztucznie podnoszą cenę kryptowaluty, aby potem szybko ją sprzedać.

Oszustwa związane z wynajmem nieruchomości: Oszust publikuje atrakcyjne oferty wynajmu mieszkań lub domów, które są zdecydowanie poniżej rynkowej stawki. Gdy ofiara wyraża zainteresowanie, oszust wymaga zapłaty z góry, zanim jeszcze ofiara zobaczy nieruchomość, często pod pretekstem, że jest za granicą i nie może pokazać nieruchomości osobiście.

Oszustwa związane z podatkami: Oszust twierdzi, że dzwoni z Urzędu Skarbowego lub innego organu podatkowego, i żąda natychmiastowej zapłaty domniemanego długu podatkowego, często pod groźbą dodatkowej kary administracyjnej.

Oszustwa techniczne: Oszust twierdzi, że dzwoni z firmy technologicznej, takiej jak Microsoft lub Apple, i informuje ofiarę, że jej komputer jest zainfekowany wirusem. Oszust prosi ofiarę o udostępnienie zdalnego dostępu do komputera lub o zapłatę za usługę techniczną.

Fałszywe wiadomości o infekcji wirusem: Szczególnie popularne podczas pandemii COVID-19, gdzie ofiary otrzymywały e-maile informujące, że były narażone na wirusa i muszą kliknąć link, aby zobaczyć więcej informacji. Link prowadził do złośliwej strony lub pliku.

Oszustwa związane z tożsamością celebrytów: Oszuści tworzą fałszywe konta na mediach społecznościowych, udając znane osoby, a następnie żądają od fanów pieniędzy lub darowizn.

Oszustwa związane z inwestycjami: Oszuści oferują „zbyt dobre, aby były prawdziwe" możliwości inwestycyjne, które obiecują niewiarygodnie wysokie zwroty.

Oszustwa związane z datingiem online: Oszust tworzy fałszywy profil na stronie randkowej i nawiązuje romans z ofiarą, tylko po to, aby później poprosić o pieniądze z różnych powodów, takich jak nagła „choroba" lub „awaria samochodu".

Oszustwa związane z kredytami studenckimi: Oszust twierdzi, że może pomóc w zlikwidowaniu lub zmniejszeniu długu z tytułu kredytów studenckich za opłatą. W rzeczywistości nie ma on takiej możliwości, a płatności często znikają.

Oszustwa związane z fałszywymi organizacjami charytatywnymi lub działaniami dobroczynnymi: Oszust prosi ofiarę o pomoc w przekazaniu pieniędzy lub darowizn na rzekomo szczytną przyczynę, ale w rzeczywistości środki trafiają do oszusta.

Schematy piramidowe lub marketingu wielopoziomowego: Oszust oferuje możliwość zarobienia dużych pieniędzy poprzez rekrutowanie nowych członków do programu. Często wymaga to od ofiary zapłaty dużej sumy z góry.

Oszustwa związane z fałszywymi pożyczkami: Oszust oferuje ofierze pożyczkę, ale wymaga „opłaty z góry" przed jej udzieleniem. Po zapłaceniu opłaty, pożyczka nigdy nie jest udzielana.

Oszustwa związane z fałszywym wsparciem technicznym: Oszust twierdzi, że jest przedstawicielem firmy technologicznej i oferuje pomoc w rozwiązaniu problemu, który nie istnieje. Mogą oni próbować zdobyć dostęp do komputera ofiary, wymagać zapłaty za usługę lub zainstalować złośliwe oprogramowanie.

Oszustwa związane z fałszywymi polisami ubezpieczeniowymi: Oszust oferuje tanią polisę ubezpieczeniową, ale po zapłaceniu składki, polisa nie istnieje lub nie oferuje obiecanych korzyści.

Oszustwa związane z ofertami podróży: Oszust oferuje atrakcyjne oferty podróży, które po zapłaceniu okazują się nieistniejące lub nie takie, jak obiecano.

Pamiętaj, że zawsze należy być ostrożnym podczas korzystania z Internetu, a zwłaszcza podczas przekazywania swoich danych osobowych lub finansowych.