Biuletyn Bezpieczeństwa Komputerowego

Oszustwa podszywające się pod zbiórki

Cyberprzestępcy wiedzą, że jednym z najlepszych sposobów nakłonienia ludzi do popełnienia błędu jest wywołanie poczucia obowiązku. Jednym z najłatwiejszych sposobów na stworzenie takiego uczucia jest wykorzystanie kryzysu. Właśnie dlatego cyberprzestępcy za każdym razem wykorzystują wydarzenie o globalnym zasięgu. To, co większość z nas uważa za tragedię, cyberprzestępcy postrzegają jako szansę na kolejne oszustwa. Przykładem może być wybuch wojny, klęska żywiołowa i oczywiście globalna pandemia, taka jak COVID-19. Gdy w wiadomościach i mediach społecznościowych pojawiają się informacje o danym wydarzeniu, cyberprzestępcy wiedzą, że nadszedł czas, aby uderzyć.

Korzystają z okazji, aby stworzyć wiadomości phishingowe lub inne oszustwa dotyczące danego wydarzenia. Następnie wysyłają wiadomości phishingowe lub tworzą kampanię uderzającą w dużą grupę ludzi. Na przykład podczas klęski żywiołowej mogą udawać organizację charytatywną, prosząc o darowizny na ratowanie potrzebujących. Cyberprzestępcy często mogą działać w ciągu kilku godzin od pierwszych wzmianek dotyczących kryzysu lub katastrofy. Mają przygotowaną całą infrastrukturę techniczną i na takie działania są gotowi z wyprzedzeniem. Jak się przed tym zabezpieczyć w momencie kolejnego globalnego kryzysu lub katastrofy?

Jak wykrywać i bronić się przed tymi oszustwami

Kluczem do uniknięcia tych oszustw jest bycie czujnym wobec każdego, kto się z nami kontaktuje. Nie ufaj wiadomościom od rzekomych organizacji charytatywnych, które pilnie potrzebują darowizn. Nawet jeśli e-mail wydaje się być wysłany przez organizację, którą znasz i której ufasz. Zachowaj czujność, jeśli odbierzesz telefon od kogoś, kto twierdzi, że jest lokalnym bankiem żywności i namawia do przekazania darowizny. Im większe poczucia obowiązku, tym większe prawdopodobieństwo ataku. Oto kilka najczęstszych wskazówek świadczących o tym, że możesz mieć do czynienia z oszustwem:

- Bądź bardzo czujny wobec wszelkich organizacji charytatywnych, które wymagają darowizny za pośrednictwem kryptowaluty, przelewów pieniężnych lub kart podarunkowych.
- Cyberprzestępcy mogą zmienić identyfikator dzwoniącego, aby połączenie wyglądało tak, jakby pochodziło z Twojej okolicy lub z zaufanej firmy. W dzisiejszych czasach nie można polegać na identyfikatorze dzwoniącego.
- Niektórzy cyberprzestępcy używają nazw i logo, które wyglądają jak prawdziwa organizacja charytatywna. To jeden z powodów, dla których przed przekazaniem pieniędzy, należy sprawdzić organizację.
- Cyberprzestępcy często w niejasny lub wzbudzający współczucie sposób opowiadają o tym, co zrobią ze zdobytymi pieniędzmi. Zazwyczaj nie podają jednak szczegółów, jak ta darowizna zostanie wykorzystana.

- Nie zakładaj, że prośby o pomoc w portalach społecznościowych, takich jak TikTok, są uzasadnione, zwłaszcza w obliczu kryzysu lub tragedii.
- Niektóre przestępstwa opierają się na podziękowaniu za darowiznę złożoną w przeszłości, mimo że taka sytuacja nie miała nigdy miejsca.
- Nie podawaj danych osobowych ani danych kart płatniczych w odpowiedzi na podejrzane wiadomości.

Jak bezpiecznie dokonać zmian

Aby przekazać darowiznę poszkodowanym, przekazuj darowizny tylko na rzecz dobrze znanych, zaufanych organizacji. Weryfikuj organizacje, na które chcesz wpłacić pieniądze. jeśli masz podejrzenia, że to oszustwo, możesz to zrobić telefonicznie, dzwoniąc do prawdziwej fundacji, która rzekomo organizuje zbiórkę. Rozważając darowiznę na cele charytatywne, wyszukaj jej nazwę oraz słowa, takie jak „skarga", „recenzja", „ocena" lub „oszustwo". Nie wiesz, którym organizacjom charytatywnym zaufać? Zacznij od wyszukania zaufanych witryn lub linków dostarczonych przez znaną i zaufaną organizację. Zbiórki na cele charytatywne to świetny sposób, aby mieć wpływ na poprawę czyjegoś życia, jednak musisz się upewnić, że przekazujesz je legalnym organizacjom.

Redaktor gościnny

Dr Jessica Barker jest wielokrotnie nagradzaną liderką bezpieczeństwa. Jest jednym z prezesów Cygenta i autorką bestsellerów. Jessica jest członkiem rady doradczej SANS Security Awareness Summit.

Źródła

Oszustwa charytatywne: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Najpopularniejsze oszustwa w mediach społecznościowych: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Wykryj i zatrzymaj ataki w wiadomościach tekstowych: ttps://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/
Nawigator charytatywny: https://www.charitynavigator.org/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz