**Uważaj na swoje sieci społecznościowe. To jeden z głównych celów cyberprzestępców**

**30 czerwca obchodzony był Dzień Mediów Społecznościowych. Słynne platformy zyskują na popularności i użytkownikach z minuty na minutę. Dziś jest łącznie 4,2 miliarda użytkowników sieci społecznościowych na całym świecie, co oznacza wzrost rok do roku o ponad 13% (490 milionów nowych użytkowników). .**

Niestety, eksperci z firmy Check Point Software Technologies ostrzegają przed niebezpieczeństwem stwarzanym przez cyberataki mające na celu kradzież kont, ze względu na ogromną wartość zapisanych na nich informacji dla cyberprzestępców. Z tego powodu eksperci z Check Point Software chcą zwrócić uwagę na różne techniki stosowane przez te osoby, aby odnieść sukces w uzurpowaniu sobie kont w mediach społecznościowych w celu ostrzeżenia użytkowników o niebezpieczeństwie:

**• Fałszywa strona internetowa:** Jedną z najczęstszych technik stosowanych przez cyberprzestępców jest fałszowanie oficjalnej strony internetowej w celu przeprowadzenia oszukańczego działania. Fałszywa strona internetowa powiela projekt oryginału, nawet używając podobnego adresu URL, co bardzo utrudnia użytkownikowi wykrycie oszustwa. Zwykle podejmuje się próbę nakłonienia ofiary do kliknięcia fałszywego linku, zwykle za pośrednictwem wiadomości SMS od znanej marki, aby wzbudzić zaufanie odbiorcy. Żąda sprawdzenia tożsamości lub ostrzega ich, że ktoś próbuje włamać się na ich konto, aby mogli wprowadzić swoje osobiste dane logowania i wykorzystać je na swoją korzyść.

**• Przejęcie DNS:** Ta metoda polega na podszywaniu się pod adres e-mail dowolnej zaufanej sieci społecznościowej w celu zdobycia danych osobowych ofiary poprzez oszustwo, które później zostaną wykorzystane do złośliwych celów. Jeśli cyberprzestępcy zdoła zdobyć dane z sieci społecznościowych danej osoby, mogą one zostać sprzedane w Dark Web i wykorzystane do rozsyłania masowych wiadomości spamowych lub łańcuchów oszustw lub innych oszustw.

**• Zainfekowany router:** Innym systemem, przez który cyberprzestępcy mogą dostać się do komputerów, a tym samym na konta użytkowników, jest infekowanie ich złośliwym oprogramowaniem, które umożliwia im dostęp do routera ofiary. Po wejściu do routera są w stanie zmodyfikować jego DNS, dzięki czemu, gdy ofiara spróbuje uzyskać dostęp do określonej strony internetowej ze swojej przeglądarki, zostanie przeniesiona na inną stronę wybraną przez atakującego. W ten sposób przestępca po raz kolejny ma jasną ścieżkę do zdobycia wszystkich danych zaatakowanego użytkownika i wykorzystania ich na swoją korzyść.

Wskazówki, jak uniknąć kradzieży danych z sieci społecznościowych

**1. Sprawdź adres URL:** Bardzo ważne jest, aby dokładnie sprawdzić adres URL, do którego chcesz uzyskać dostęp, aby zidentyfikować różnice z oryginałem, a tym samym uniknąć wpadnięcia w pułapkę. Kolejnym szczegółem, na który należy zwrócić uwagę, jest to, że strona internetowa ma certyfikat SSL. Technologia ta zapewnia bezpieczeństwo połączenia internetowego i chroni wszelkie poufne informacje przesyłane między dwoma systemami oraz uniemożliwia cyberprzestępcom przeglądanie i modyfikowanie wszelkich przesyłanych danych, w tym informacji, które mogą zostać uznane za osobiste. Jest rozpoznawany na początku samego adresu URL poprzez dodanie „s” na początku akronimu https://.

**2. Nigdy nie klikaj linków:** Gdy otrzymasz wiadomość e-mail lub SMS z dowolnego e-maila z sieci społecznościowej, zaleca się, aby nigdy nie klikać linku, jeśli jest złośliwy. Zaleca się skorzystanie z wyszukiwarki, aby przejść do strony internetowej firmy, którą piszesz, aby uniknąć możliwego oszustwa.

**3. Nigdy nie udostępniaj danych osobowych:** Kradzież informacji jest częstym celem cyberprzestępców. Wiele osób bardzo często używa tych samych nazw i haseł na różnych kontach w mediach społecznościowych, więc kradzież danych z jednego daje atakującemu możliwość zrobienia tego na innych. Nie udostępnianie danych osobowych i nieużywanie tego samego hasła to jeden z najlepszych sposobów ochrony.

**4. Zawsze uważaj na wiadomości e-mail sugerujące zmianę hasła:** Jeśli otrzymasz niechcianą wiadomość e-mail z prośbą o zmianę hasła, koniecznie przejdź bezpośrednio do strony (nie klikaj linku w wiadomości e-mail) i odnów hasło od tę samą stronę (i z innych kont, na których masz tę samą). Brak hasła to jeden z problemów, z jakimi borykają się cyberprzestępcy, próbując uzyskać dostęp do konta internetowego. Aby go zdobyć, wysyłają użytkownikowi fałszywy e-mail, aby go zmienić, przekierowują go na stronę phishingową, a tam proszą o podanie swoich danych osobowych i podanie ich do ich celów.

**5. Zwróć uwagę na język:** gdy atakujący wysyła wiadomość e-mail podszywającą się pod tożsamość dowolnej sieci społecznościowej, zwróć szczególną uwagę na używany język. Ważne jest, aby szukać ewentualnych błędów ortograficznych w e-mailach lub na stronach internetowych, ponieważ znalezienie „o” w miejscu, w którym powinno być zero, lub błędna pisownia nazwy firmy to jeden ze znaków, który powinien uruchomić wszystkie dzwonki alarmowe.