F-Alert

Miesięczny raport o zagrożeniach

F-Secure

Październik 2023

F-Secure

Odkryj najnowsze informacje dotyczące zagrożeń. Zawiera szczegółowe opracowania od ekspertów z firmy F-Secure. Dostarczane co miesiąc.

Poznaj niebezpieczeństwo kryjące się za niektórymi kodami QR. Zobacz, dlaczego Google chce, abyś zapomniał(a) swoich haseł. Odkryj, co może robić urządzenie Android TV podczas oglądania Netflixa. I dowiedz się, dlaczego większość oszustw zakupowych zaczyna się od reklam na Facebooku. Wszystko to i jeszcze więcej w tym miesiącu w F-Alert.

Joel Latto
Doradca ds. zagrożeń
Helsinki, Finlandia

porada experta

To świetnie, że iOS, na przykład, pokazuje podgląd linku podczas odczytywania kodu QR. Ale pokazuje tylko częściowy link. Nadal potrzebujesz ochrony przeglądania, aby chronić się przed złymi adresami URL, które mogą wywoływać kody QR.

“Kody QR mogą obejść ochronę przed spamem łatwiej niż zwykły phishing”.

QR phishing wchodzi do głównego nurtu

Ataki wykorzystujące kody QR do kradzieży danych uwierzytelniających stały się tak powszechne, że zyskały przydomek - quishing.

Pierwsze kody QR zostały zaprojektowane w 1994 roku. Jednak wielu użytkowników Internetu poznało je dopiero niedawno, kiedy technologia ta została przyjęta przez wiodące aplikacje do uwierzytelniania dwuskładnikowego oraz jako bezdotykowe narzędzie cyfrowe podczas pandemii Covid-19.

Cyberprzestępcy oczywiście nigdy nie przegapią okazji. W październiku 2023 r. AT&T ostrzegła przed "quishingiem" ponieważ wyszukiwania "QR code phishing" osiągnęły rekordowy poziom.

Nieco wyjątkowe zagrożenie

Niektórzy specjaliści ds. cyberbezpieczeństwa debatują nad tym, czy ”quishing” istnieje, czy też jest to po prostu zbyt uroczy sposób opisania innej formy phishingu, jednego z najczęstszych zagrożeń, z którymi spotykają się użytkownicy.

Istnieją jednak wyjątkowe aspekty zagrożeń wynikających ze skanowania kodów, których konsumenci muszą być świadomi, wyjaśnia Joel Latto, doradca ds. zagrożeń w F-Secure.

”Kody QR mogą ominąć ochronę przed spamem łatwiej niż zwykły phishing, ponieważ sama wiadomość e-mail nie musi zawierać żadnych linków wychodzących, które mogłyby spowodować wykrycie” - powiedział. ”Mogą być również wykorzystywane do inicjowania pobierania złośliwych aplikacji lub plików, zwłaszcza na telefonach”.

Na wolności

Oszustwa związane z kodami QR są również wyjątkowe, ponieważ użytkownicy mogą się na nie natknąć zarówno w Internecie, jak i poza nim, dodał Latto, który od lat ostrzega przed niebezpieczeństwami związanymi z kodami QR “na wolności”.

W ubiegłym roku FTC ostrzegła konsumentów przed oszustwem w Teksasie, które rozpoczęło się od złośliwych kodów QR na parkometrach.

“Naprawdę jedynym ograniczeniem jest tutaj wyobraźnia przestępców” podsumował.

Popularne Oszustwa

“Phantom Hacker” niszczy seniorów

CO:
The FBI ostrzega przed trójfazowym oszustwem, które przyniosło ponad pół miliarda dolarów strat tylko w pierwszej połowie 2023 roku, często atakując seniorów i zabierając wszystko, co mają. Oszustwo to przypomina tradycyjne oszustwo związane z pomocą techniczną i przekształca się w przestępców udających urzędników bankowych lub rządowych, którzy nalegają, aby ofiary przelały duże sumy pieniędzy na różne konta w celu “bezpiecznego” przechowywania.

JAK:
Wykorzystując wiedzę na temat kont finansowych, do których ofiara uzyskała dostęp za pośrednictwem urządzenia, przestępcy wysuwają konkretne żądania przesłania środków za granicę za pośrednictwem przelewu bankowego, gotówki lub kryptowaluty, jednocześnie nalegając, aby transakcje były utrzymywane w tajemnicy.

PRZYGOTUJ SIĘ:
1) nigdy nie ulegaj prośbie o pobranie oprogramowania od kogokolwiek, kto się z Tobą skontaktował i 2) natychmiast zatrzymaj się i poszukaj pomocy, jeśli nieznajomy powie Ci, abyś nikomu nie mówił o tym, o co Cię prosi.

Naruszenie, które ma znaczenie

23andMe

DLACZEGO MA TO ZNACZENIE:
Dane użytkowników z co najmniej 835 000 klientów 23andMe pojawiły się na forum internetowym na początku października. Witryna z testami genetycznymi potwierdziła, że jej oferta “DNA Relatives” została “naruszona”.

NARUSZONE DANE:
Dane zawierają imiona i nazwiska, daty urodzenia, kraj, adresy e-mail i inne dane osobowe. Wyjątkowe w tym wycieku jest to, że dane zostały zidentyfikowane i pogrupowane według pochodzenia etnicznego – w szczególności Żydów aszkenazyjskich i pochodzenia chińskiego.

CO NALEŻY ZROBIĆ:
Wszyscy użytkownicy 23andMe powinni upewnić się, że ich hasło jest silne i unikalne oraz aktywować uwierzytelnianie dwuskładnikowe. EFF sugeruje, że użytkownicy mogą chcieć pobrać swoje dane z witryny i usunąć swoje konta lub przynajmniej rozważyć konsekwencje powierzenia stronie trzeciej danych dotyczących DNA, które zawierają wszystkie informacje genetyczne.

Czy Twoje dane zostały ujawnione online?
Sprawdź za pomocą naszego narzędzia
F-Secure Identity Theft Checker!

Google wprowadza klucze dostępu

Gigant technologiczny zachęca teraz wszystkich użytkowników do porzucenia haseł na rzecz odcisku palca, skanu twarzy, pinu lub wzoru.

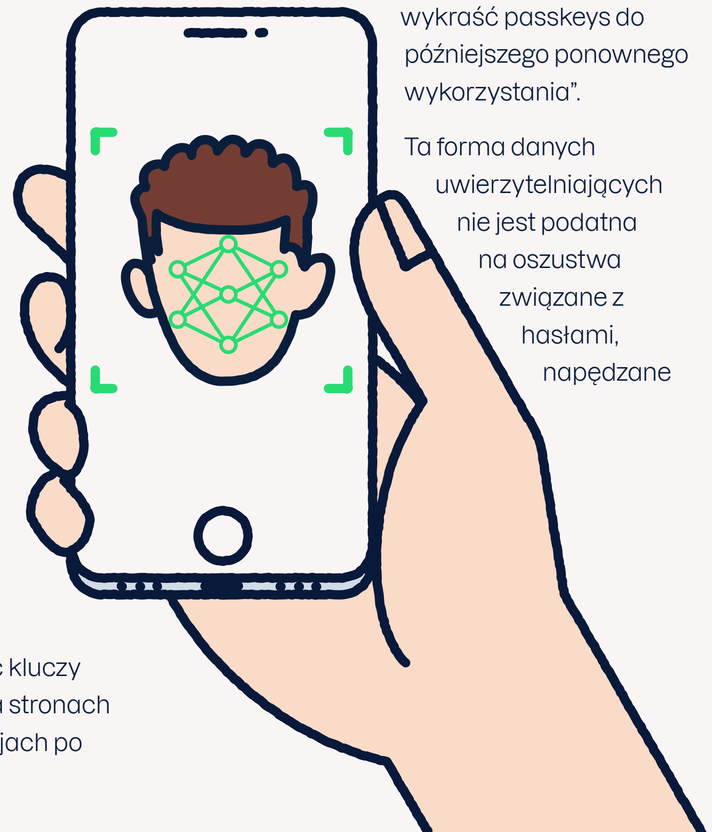
Są bezpieczniejsze niż hasła. Nie trzeba ich zapamiętywać. I są o 40% szybsze. .

To argument Google dlaczego klucze dostępu zastąpiły hasła jako domyślny sposób zabezpieczania kont na platformie. Ten krok z okazji Miesiąca Świadomości Cyberbezpieczeństwa jest najnowszym sygnałem, że liderzy branży nadal poważnie podchodzą do zakończenia ery haseł.

Nie można użyć ponownie

Ash Shatrieh, F-Secure Threat Intelligence Researcher, zbadał protokół passkey i zgadza się, że są one lepszą opcją niż hasła - z niemal każdego powodu.

“Użytkownicy mogą używać kluczy dostępu do logowania się na stronach internetowych lub w aplikacjach po prostu za pomocą uwierzytelniania biometrycznego urządzenia, takiego jak odcisk palca lub skan twarzy" - powiedział. "Passkeys są powiązane ze stroną internetową; oznacza to, że fałszywe strony internetowe nie mogą wykraść passkeys do późniejszego ponownego wykorzystania”.



Ta forma danych uwierzytelniających nie jest podatna na oszustwa związane z hasłami, napędzane ciągłymi naruszeniami danych lub phishingiem.

Liczne zalety, ale nie doskonałość

“Zmiana w kierunku świata bez haseł oferuje liczne korzyści w zakresie bezpieczeństwa, ale nie jest jeszcze idealna" - powiedział Ash. "Sposób, w jaki klucze muszą być synchronizowane z chmurą użytkownika, oznacza, że proces odzyskiwania konta jest nadal otwarty na ataki phishingowe”.

Google wdrożyło klucze dostępu w ramach sojuszu FIDO w celu wyeliminowania haseł na początku tego roku. Wielu członków FIDO - w tym Amazon, Apple i Microsoft - wdrożyło już obsługę kluczy dostępu. “Kiedy największa na świecie firma zajmująca się wyszukiwaniem i reklamą wprowadza coś domyślnego, inni zwykle podążają za nią” - podsumował Ash.

Ash Shatrieh
Badacz ds. analizy zagrożeń
Helsinki, Finlandia

porada experta

Krajobraz zagrożeń przesunie się w kierunku phishingu związanego z odzyskiwaniem kont, a nie zostanie całkowicie wyeliminowany. Bezpieczeństwo tożsamości użytkowników pozostaje tak dobre, jak procesy odzyskiwania ich kont.

“Przejście na świat bez haseł oferuje liczne korzyści w zakresie bezpieczeństwa, ale nie jest jeszcze idealne”.

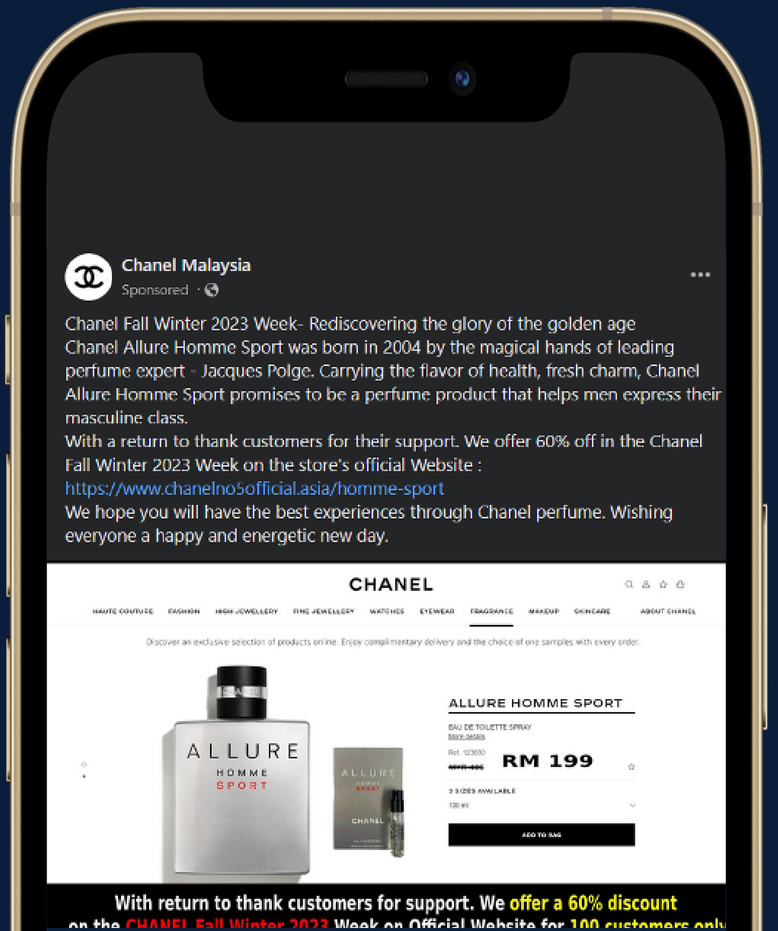
Jak działają oszustwa zakupowe na Facebooku

Oszustwa związane z zakupami stają się coraz powszechniejsze dzięki platformom mediów społecznościowych, które reklamują niemal wszystko.

Jeśli możesz stracić pieniądze w wyniku oszustwa, istnieje duże prawdopodobieństwo, że oszustwo rozpocznie się w mediach społecznościowych.

A jeżeli możesz zostać oszukany w mediach społecznościowych, jednym z głównych powodów jest to, że platformy te są wypełnione reklamami przedstawiającymi fałszywe produkty z fałszywymi rabatami.

44% wszystkich zgłoszeń o oszustwach w mediach społecznościowych pochodziło od osób, które próbowały kupić coś reklamowanego w mediach społecznościowych. Podobne do tego:

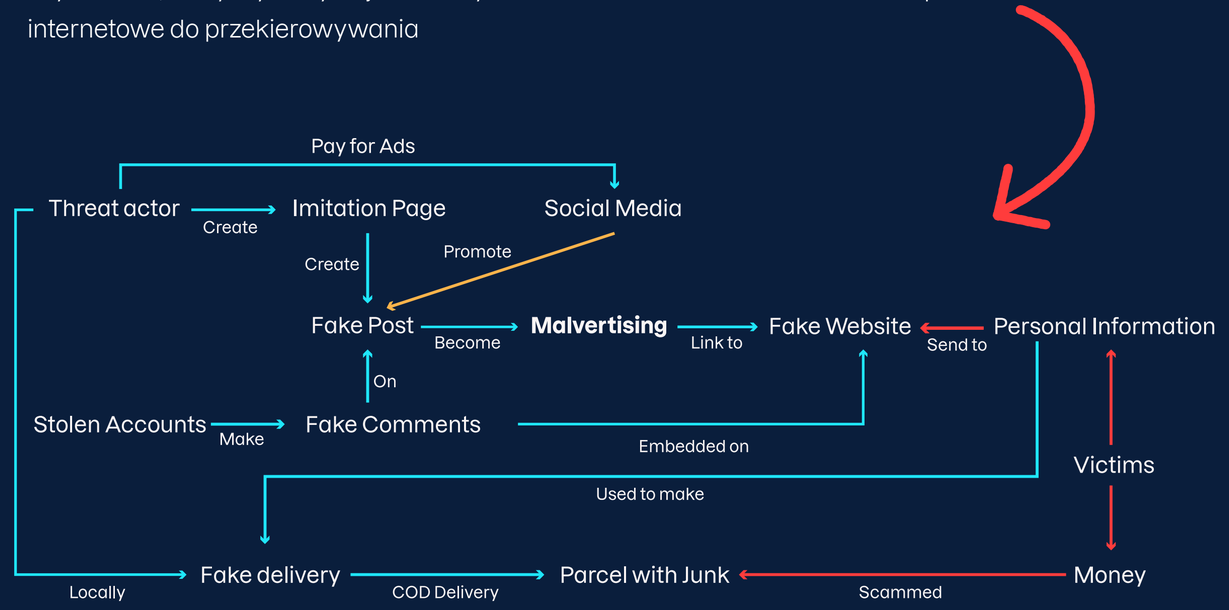


Najczęstsze oszustwa zakupowe kończyły się tym, że zakupione towary nigdy nie docierały lub były podmieniane na śmieci.

Ten rodzaj oszustwa jest znany jako Malvertising. Co to jest?

“Cyberatak, który wykorzystuje reklamy internetowe do przekierowywania konsumentów do złośliwych witryn i aplikacji" - powiedział Yik Han, badacz z firmy F-Secure, który znalazł powyższy przykład.

Poprosiliśmy Yik Hana o przedstawienie, w jaki sposób to cyberprzestępstwo stało się biznesem wartym miliardy dolarów. Wymyślił to niesamowite wizualne podsumowanie:



Krótka wersja?

Oszuści zakładają fałszywe strony na Facebooku imitujące marki, które lubisz, a następnie tworzą fałszywe posty, które są promowane jako reklamy i dodatkowo wzmacniane fałszywymi komentarzami, które następnie prowadzą do fałszywych stron internetowych, które naciskają na zakup czegoś, co nigdy nie dotrze.

Następnie wykorzystują te pieniądze, aby kupić więcej reklam i oszukać więcej osób.

Yik Han
Badacz
Puchong, Malezja

porada experta

"W dzisiejszych czasach łatwo jest podrobić wszystko w mediach społecznościowych. Dlatego przed dokonaniem zakupu należy sprawdzić, czy sprzedawca internetowy jest legalny, korzystając z narzędzia takiego jak F-Secure’s Online Shopping Checker”.

Mika Lehtinen
Dyrektor ds.
współpracy badawczej
Helsinki, Finlandia

porada experta

Kupując sprzęt z Androidem, przyjrzyj się uważnie najnowszym recenzjom i staraj się trzymać urządzeń z certyfikatem Play Protect. Żadne z uszkodzonych urządzeń nie było certyfikowane przez Play Protect.

“Tajemnicą pozostaje, kiedy zainstalowano backdoory w oprogramowaniu układowym”.

Backdoory w systemie Android TV wykorzystane

Popularne urządzenia streamingowe z zainstalowanym złośliwym oprogramowaniem wydają się dokonywać oszustw.

Podczas gdy ty oglądasz telewizję, twoje tanie urządzenie do streamingu z Androidem może popełniać przestępstwa.

Raport z początku tego roku wykazał, że urządzenia Android TV od chińskich producentów mogą być instalowane z aktywnym złośliwym oprogramowaniem. Teraz nowe dowody sugerują, że urządzenia z setek modeli Androida zostały włączone do sieci urządzeń zombie w celu popełniania oszustw.

Sprzedawane na głównych stronach internetowych

“Raport zidentyfikował 77 000 urządzeń z backdoorami, które otwierają je na instalację złośliwego oprogramowania, ale prawdopodobnie na całym świecie sprzedawane są miliony takich urządzeń”. - powiedział Mika Lehtinen, dyrektor ds. współpracy badawczej w F-Secure. “Na rynku są miliony podobnych urządzeń”.

Dotknięte modele zostały dostarczone klientom zainfekowane wyrafinowanym i elastycznym złośliwym oprogramowaniem znanym jako Triada, które otrzymywało aktywne "moduły" oszustwa, gdy tylko urządzenia zostały włączone.

“Najbardziej znaczące jest to, że sprzęt ten jest sprzedawany za pośrednictwem popularnych witryn e-commerce, takich jak Amazon” - powiedział Lehtinen. “Tajemnicą pozostaje, kiedy zainstalowano backdoory w oprogramowaniu układowym”.

Klienci w ciemności

Oszustwa reklamowe, fałszywe wiadomości e-mail i przejęte proxy oraz instalacja kodu przez zainfekowane skrzynki odbywają się po cichu..

“Jedynym sygnałem, że urządzenie uczestniczy w globalnym botnecie zorganizowanej przestępczości, mogą być niewielkie problemy z wydajnością” - powiedział. “Ale ponieważ te urządzenia są zainfekowane od momentu ich uruchomienia, szanse na to, że klient to zauważy, są niewielkie”.

Bezpieczeństwo w internecie z F-Secure

- Ochrona kont bankowych i płatności w sieci
- Ochrona antywyłudzeniowa, która blokuje wejścia na fałszywe strony
- Blokowanie podrobionych aplikacji, które mogą służyć do wykradania danych
- Limit czasu przed ekranem i pora spać, aby dzieci zdrowo korzystały z telefonów

Ochrona tożsamości od F-Secure

- Monitorowanie wycieków danych do internetu
- Natychmiastowe alerty z poradami krok po kroku co zrobić w kryzysowej sytuacji
- Pomoc w tworzeniu mocnych i unikalnych haseł

F-Secure