RATE HAWK

Świadomość phishingu: jak chronić swoje konto przed zagrożeniami online?

Czy czasami otrzymujesz podejrzane e-maile zachęcające do kliknięcia jakiegoś linku? Istnieje duże prawdopodobieństwo, że jest to phishing. Aby chronić swoje dane i wyprzedzać potencjalne zagrożenia, najważniejsza jest świadomość i podejmowanie proaktywnych działań. W tym artykule zagłębimy się w skuteczne kroki w zakresie cyberbezpieczeństwa i omówimy środki, które należy podjąć podczas pracy z naszą platformą.

1 Phishing w liczbach: zrozumienie zagrożenia

15%
wszystkich naruszeń danych wynika z phishingu (raport IBM).

$52M+
strat zgłoszonych w USA z powodu phishingu (FBI IC3, 2022)

300k
ofiar zgłoszonych w USA w 2022 roku.

Ataki phishingowe nasilają się, zagrażając osobom fizycznym i firmom na całym świecie. Według raportu IBM phishing jest najczęstszą formą naruszenia danych, stanowiącą 15% wszystkich incydentów. Równie alarmujące są straty finansowe: dane z Centrum Zgłaszania Przestępstw Internetowych FBI (IC3) ujawniają, że ataki phishingowe były najczęściej zgłaszanym przestępstwem w USA w 2022 r. – zgłoszono 300 497 ofiar i poniesiono straty przekraczające 52 mln USD.

Branża turystyczna nie jest tu wyjątkiem. Raport sporządzony przez Grupę Roboczą ds. Zwalczania Phishingu (APWG) ujawnił, że branża turystyczna znalazła się w pierwszej dziesiątce najczęściej atakowanych sektorów. Forbes ostrzega, że wraz z postępującą integracją technologii z doświadczeniami związanymi z podróżowaniem, ryzyko cyberataków podczas rezerwacji podróży lub uzyskiwania dostępu do niezabezpieczonych sieci za granicą staje się coraz poważniejsze.

Dlaczego więc branża turystyczna jest głównym celem ataków? Platformy rezerwacji online przetwarzają ogromne ilości wrażliwych danych – od danych osobowych po informacje finansowe – co stanowi atrakcyjny łup dla cyberprzestępców. Należy jednak pamiętać, że phishing to problem globalny, który wpływa na cały ekosystem online – nie odzwierciedla on bezpieczeństwa naszej platformy. W celu ochrony naszych użytkowników wdrażamy zaawansowane środki bezpieczeństwa, które w połączeniu ze świadomością pomagają zapewnić najwyższy poziom ochrony.

2 Jak działa phishing?

Phishing to forma cyberataku, w której oszuści podszywają się pod legalne podmioty, aby nakłonić użytkownika do ujawnienia poufnych informacji. Dokonujący ataku często posługują się wiadomościami e-mail, wiadomościami tekstowymi lub fałszywymi witrynami internetowymi, które wiernie imitują autentyczne źródła. Oto jak zazwyczaj działa phishing:

Fałszywe strony logowania:
cyberprzestępcy tworzą fałszywe strony internetowe, które wyglądają identycznie jak oficjalne strony logowania. Niewielka różnica, taka jak dodatkowa litera lub drobna zmiana adresu URL, może wprowadzić w błąd nawet najbardziej ostrożnych użytkowników.

Oszukańcze oferty:
wiadomości e-mail lub SMS-y phishingowe często zawierają pilne lub kuszące sformułowania, nakłaniające do kliknięcia linku lub podania danych logowania. Często posługują się pilnymi ofertami, jak np. zniżki, oferty specjalne lub ograniczone czasowo promocje, aby nakłonić do kliknięcia przesyłanych linków. Ich celem jest zdobycie danych osobowych użytkownika, zanim ten zorientuje się, co się właściwie dzieje.

Złośliwe reklamy:
wchodząc na stronę internetową należy pamiętać, że nie wszystkie reklamy są godne zaufania. Przed i po kliknięciu reklamy należy zawsze dokładnie sprawdzić adres URL, aby upewnić się, że jest się na legalnej stronie. Oszuści często wykorzystują wprowadzające w błąd reklamy, aby kierować użytkowników na fałszywe strony, które wyglądają na prawdziwe, ale mają na celu kradzież informacji.

Zrozumienie i świadomość tych taktyk to pierwszy krok do ochrony siebie i swojej firmy.

3 Kroki mające na celu ochronę konta przed atakami phishingowymi

Wdrożenie kilku prostych praktyk może znacznie przyczynić się do zabezpieczenia kont i zapobiegania atakom phishingowym:

Sprawdź dokładnie adres URL:
zawsze sprawdzaj, czy jesteś na stronie www.ratehawk.com. Nieuczciwe witryny często mają niewielkie różnice w adresie URL (np. ratehwak.com zamiast ratehawk.com).

Unikaj klikania podejrzanych linków:
jeśli otrzymasz nieoczekiwaną wiadomość e-mail lub SMS-a z prośbą o zalogowanie się, nie klikaj podanego linku. Zamiast tego przejdź bezpośrednio na stronę www.ratehawk.com/accounts/login.

Nigdy nie udostępniaj swoich danych logowania:
pracownicy RateHawk nigdy nie proszą o podanie loginu lub jednorazowego hasła za pośrednictwem poczty elektronicznej, telefonu ani mediów społecznościowych. Jeśli otrzymasz taką prośbę, natychmiast ją zgłoś.

Używaj silnych i unikatowych haseł:
utwórz bezpieczne hasło, posługując się kombinacją liter, cyfr i symboli. Unikaj wielokrotnego używania tych samych haseł na różnych kontach. Stosowane hasła powinny być unikatowe dla każdej z platform. Jeśli naruszony zostanie dostęp do jednego z serwisów, wielokrotne używanie tego samego hasła może narazić inne konta na poważne ryzyko.

Regularnie aktualizuj hasło:
zmiana hasła co kilka miesięcy zmniejsza ryzyko nieautoryzowanego dostępu.

Wprowadzając te praktyki do swojej codziennej rutyny, można stworzyć solidną obronę przed atakami phishingowymi, a w rezultacie chronić swoje dane osobowe. Wzmocnij swoje bezpieczeństwo dzięki tym prostym krokom i śpij spokojnie z RateHawk!