Bezpieczeństwo użytkowników na portalu Uprawnienia-budowlane.pl

Phishing – co to takiego?

Phishing, nazywany również spoofingiem, to działania mające na celu wyłudzenie poufnych informacji od użytkownika internetu. Mogą to być informacje dotyczą loginów i haseł do logowania, numerów kart kredytowych oraz innych wrażliwych danych personalnych. W celu dokonania tego wyłudzenia, oszust podszywa się pod inną osobę, firmę bądź instytucję. Najczęstsze metody phishingu stosowane w internecie to tworzenie fałszywych stron www imitujących oryginalne adres – np. stron logowania do kont bankowych, jak również rozsyłanie fałszywych wiadomości e-mail.

Jakich pytań nigdy nie zada konsultant?

1. Pytanie o hasło – nigdy i żaden konsultant Uprawnienia-budowlane.pl nie zapyta użytkownika o hasło do jego konta. Jest ono znane wyłącznie użytkownikowi serwisu.

2. Pytanie o kartę kredytową – a dokładnie o podanie jej pełnego numeru, kodu zabezpieczającego, daty ważności karty lub kodu Secure 3D, służącego do dodatkowej weryfikacji płatności.

Jak odróżnić prawdziwą stronę logowania od fałszywej?

1. Wejdź na stronę logowania Uprawnienia-budowlane.pl i dodaj ją do ulubionych zakładek w przeglądarce.

2. Zawsze sprawdzaj adres strony wyświetlany w górnym pasku – poprawny to https://uprawnienia-budowlane.pl.

3. Strona Uprawnienia-budowlane.pl zawsze otwiera się jako bezpieczne, szyfrowane połączenie danych – potwierdza to ikona kłódki obok adresu.

4. Strona Uprawnienia-budowlane.pl korzysta z certyfikatu GeoTrust QuickSSL Premium, który zabezpiecza komunikację pomiędzy urządzeniem użytkownika a stroną Uprawnienia-budowlane.pl.

5. Zanim się zalogujesz do swojego konta, skontroluj adres strony www, w tym prawidłowe brzmienie domeny oraz ważność i nazwę certyfikatu. Jakakolwiek różnica, np. zmieniony szyk liter może wskazywać na próbę oszustwa.

6. Nie daj się zwieść próbie podrobienia wyglądu naszej strony www. Częstym działaniem jest jej kopiowanie, tak aby podrobiona strona do złudzenia przypominała oryginał. Można to rozpoznać po subtelnych różnicach, wynikających z błędnego kodowania lub pomyłek podczas kopiowania strony. Jednak najlepszym

i najbardziej wiarygodnym sposobem na potwierdzenie autentyczności strony Uprawnienia-budowlane.pl, jest każdorazowe sprawdzanie jej adresu i certyfikatu. Można to sprawdzić w widocznym u góry okna przeglądarki pasku adresowym.

Jak odróżnić prawdziwą wiadomość e-mail od fałszywej?

1. Strona Uprawnienia-budowlane.pl nigdy nie wysyła wiadomości e-mail, w których prosi użytkowników o podanie danych dostępowych do swojego konta w serwisie lub innych poufnych danych.

2. W przypadku otrzymania wiadomości e-mail z prośbą o przekazanie jednej z niżej wymienionych danych, najprawdopodobniej jest to próba wyłudzenia danych. Przykładowe takich wiadomości to np.

- prośba o wysłanie wiadomości SMS na podany numer,
- prośba o podanie loginu i hasła do portalu Uprawnienia-budowlane.pl,
- prośba o zalogowanie się do serwisu za pomocą linku, który został umieszczony w treści wiadomości lub jej załączniku,
- prośba o podanie innych wrażliwych danych, jak data urodzenia, nr PESEL, nazwisko panieńskie matki, dane karty kredytowej.

3. Wskazówką do odróżnienia wiadomości fałszywej od prawdziwej są również możliwe błędy gramatyczne i stylistyczne, bardzo często pojawiające się w fałszywych e-mailach.

4. W wiadomościach e-mail od serwisu Uprawnienia-budowlane.pl, nigdy nie znajdują się załączniki z plikami wykonawczymi o rozszerzeniu .exe, ani jakiekolwiek inne załączniki. Nawet w przypadku otrzymania wiadomości, w której treści znajduje się dokładna instrukcja wykonania jakiejś czynności na koncie Uprawnienia-budowlane.pl, najlepszym sposobem jej wykonania będzie ręczne wpisanie adresu Uprawnienia-budowlane.pl do przeglądarki i zweryfikowanie prawidłowości adresu oraz certyfikatu. Po prawidłowym zalogowaniu się do konta, należy zweryfikować zalecane w wiadomości czynności. Dla bezpieczeństwa nie należy nigdy klikać w linki, które znajdują się w treści wiadomości, w której znajduje się prośba o przekazanie danych osobowych, danych do kont bankowych, kart płatniczych oraz wszystkich innych wiadomości, których wiarygodność budzi jakiekolwiek wątpliwości.

Phishing – jak zgłosić atak

W przypadku otrzymania fałszywej wiadomości e-mail:

1. Wyślij najlepiej całą wiadomość, wraz z jej wszystkimi nagłówkami – w tym adresem nadawcy itp. na adres naszej poczty e-mail:
biuro@uprawnienia-budowlane.pl

2. Zweryfikujemy przekazaną nam wiadomość i poinformujemy czy jest ona prawdziwa czy fałszywa. Twoje działanie może nam pomóc chronić innych użytkowników przed możliwymi wyłudzeniami i oszustwami.

Kradzież tożsamości – co to takiego

Kradzież tożsamości jest dziś coraz częstszym przestępstwem. Można go dokonać kiedy oszust wejdzie w posiadanie wrażliwych danych osobowych. Zwykle kradzione są takie informacje jak imię i nazwisko, adres zameldowania i zamieszkania, numer PESEL, numer karty kredytowej, numer i seria dowodu osobistego oraz inne dane, pozwalające oszustowi zaciągnąć na nie kredyt lub pożyczkę bądź płacić cudzą kartą kredytową za zakupy online.

Chroń swoją tożsamość – dowiedz się jak

- Zabezpiecz swoje poufne dane – tak w sieci, jak i w życiu realnym,
- Korzystaj z bezpiecznych płatności – np. systemu płatności Przelewy24.pl,
- Nie odpowiadaj na wiadomości, w których ktoś prosi o przesłanie danych logowania, numerów kart kredytowych, numeru PESEL, adresu zamieszkania i innych danych,
- Kontroluj historię konta i karty – regularnie sprawdzaj historię transakcji na swoich kontach bankowych oraz kartach płatniczych. Szukaj podejrzanych transakcji i jeśli je znajdziesz, zgłoś je obsłudze swojego banku.
- Zanim zamkniesz okno przeglądarki, pamiętaj aby wylogować się z konta, z którego aktualnie korzystałeś. Dotyczy to zarówno kont bankowych, jak i pozostałych kont internetowych, również w serwisie Uprawnienia-budowlane.pl.

Bezpieczne płatności online – o czym pamiętać

- Sprawdź certyfikat SSL – sprawdzaj czy obok adresu odwiedzanej strony internetowej widoczny jest symbol kłódki oraz czy adres rozpoczyna się od htttps://,
- Sprawdź informacje o właścicielu strony – na odwiedzanej stronie powinieneś bez trudu znaleźć takie dane jak kontakt do sprzedawcy, regulaminy, w tym regulamin zwrotów, reklamacji i politykę prywatności. Nie powinno również zabraknąć numeru telefonu do sprzedawcy.

Bezpieczny komputer – co musi posiadać

Bezpieczne korzystanie z internetu w dużej mierze opiera się na prawidłowo zabezpieczonym urządzeniu oraz legalnym i sprawdzonym oprogramowaniu. Kiedy decydujesz się na płatności online, zawsze trzeba pamiętać o:

- aktualnym programie antywirusowym,
- włączonej zaporze sieciowej – firewall,
- aktualnym oprogramowaniu.

Skuteczny antywirus chroni komputer przed szkodliwym oprogramowaniem, czyli wirusami i trojanami. Komputer może zostać nimi zainfekowany poprzez otwarcie załączników otrzymanych pocztą e-mail lub pobranie zainfekowanego programu z internetu. Programy antywirusowe przed otwarciem takich programów i plików, dokonują ich wcześniejszego skanowania w poszukiwaniu zagrożeń. Kiedy go znajdą, uniemożliwiają otwarcie takiego programu / aplikacji / dokumentu / adresu strony www.

Aby programy antywirusowe działały skutecznie i zapewniały nam maksymalną ochronę, należy pamiętać o ich regularnej aktualizacji. Ponadto komercyjne, płatne programy antywirusowe mają zwykle większą skuteczność ochrony i rozpoznają większą liczbę potencjalnych zagrożeń. Jeśli nie posiadasz jeszcze programu antywirusowego lub brakuje Ci pieniędzy na zakup pełnej wersji, zawsze możesz zainstalować darmową, próbną wersję takiego komputera. Zapewnia ona bezpieczeństwo zwykle przez 30 dni. Po tym czasie program przestaje być aktywny i chcąc z niego nadal korzystać, należy go aktywować zakupionym kluczem licencyjnym.

Zapora sieciowa, czyli firewall, zapewnia naszemu komputerowi ochronę przed nieautoryzowanym dostępem z internetu lub sieci wewnętrznej. Jest szczególnie przydatna, kiedy korzystamy z niezabezpieczonych lub darmowych sieci wifi i hotspotów, np. w barach fast food. Nie posiadając firewalla, umożliwiamy osobom z zewnątrz dostanie się do naszego komputera i podglądanie całej jego zawartości, w tym również tego, co robimy w internecie. Pozwala to poznać wysyłane przez nas dane, takie jak treści wiadomości, loginy oraz hasła.

Aktualne programy – producenci oprogramowania dokonują ich regularnej aktualizacji. Aktualizacje mają eliminować znalezione wcześniej dziury, które mogłyby być wykorzystane do ataku na komputer lub destabilizowałyby jego prawidłową pracę. Podstawą jest w tym przypadku regularnie aktualizowany system operacyjny, antywirus, program pocztowy oraz przeglądarka internetowa.