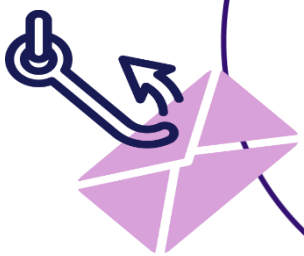
CYBERBEZPIECZEŃSTWO – BEZPIECZEŃSTWO W SIECI

W związku z rosnącymi zagrożeniami w sieci związanymi z oszustwami internetowymi, Q Securities dba o zwiększenie świadomości i wiedzy wśród swoich klientów w zakresie cyberbezpieczeństwa (ang.cybersecurity).

Bądź świadomym użytkownikiem sieci i zapoznaj się z opracowanymi przez Q Securities poniżej informacjami.

Niniejsza broszura ma charakter wyłączenie informacyjno-edukacyjny i została skierowana do klientów Q Securities S.A. (dalej „**Q Securities**").

Najczęstsze rodzaje zagrożeń w sieci:



- **Czym jest Phishing?** Nazwa pochodzi od *password* („hasło") oraz *fishing* („wędkowanie"). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się do serwisów. Po uzyskaniu dostępu pod pretekstem autoryzacji, aktualizacji danych, czy potwierdzenia odbioru przelewu lub zasilenia środków sugerują konieczność zalogowania się na fałszywej stronie, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw. Korzystający z tej metody oszuści tworzą również fałszywe strony internetowe, czy wiadomości email przypominające oryginalne strony i emaile profesjonalnych podmiotów w tym instytucji finansowych oraz firm inwestycyjnych. W tym celu przestępcy wykorzystują często logotypy organizacji, czy instytucji, kopiują wygląd, styl i szatę graficzną komunikatów tworząc fałszywe strony internetowe.

- **Jak uchronić się od Phishingu?** Bądź uważny! Sprawdzaj adres strony, na której się znajdujesz. Szczególnie, gdy wpisujesz swoje dane do logowania. Jeżeli coś wzbudzi Twoją podejrzliwość co do wyglądu panelu klienta lub strony internetowej Q Securities zawsze możesz skontaktować z naszą infolinią w celu zgłoszenia wątpliwości pod numerem telefonu + 48 22 417 44 00. Pamiętaj – Q Securities nie stosuje w kontakcie z klientami praktyki wysyłania aktywnych linków do stron internetowych za pośrednictwem wiadomości SMS lub e-mail bez uprzedniej autoryzacji.

- **Czym jest Smishing?** Smishing to rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak na przykład loginy i hasła do serwisów lub numer karty kredytowej użytkownika. Drogą ataku są wiadomości tekstowe lub SMS i stąd wzięła się nazwa – „SMiShing". Cyberprzestępcy wykorzystujący tę metodę wysyłają smsy, w których informują np. o nowej transakcji na koncie i konieczności jej potwierdzenia w podanym linku prowadzącym do fałszywej strony internetowej. Podając na niej swój login i hasło, oszuści przejmują dostęp do prawdziwych kont.

- **Jak uchronić się od Smishingu?** Bądź podejrzliwy co do treści każdego SMS-a i nigdy nie klikaj w linki wysłane w ten sposób oraz nie podawaj swoich danych osobowych oraz danych do logowania czy numeru karty kredytowej przez telefon. Zwróć uwagę jak wygląda podejrzany link, bo często nie ma o nic wspólnego z firmą, która jest rzekomym nadawcą. Pamiętaj – żaden pracownik profesjonalnego podmiotu nie powinien prosić Cię o udzielenie takich informacji. Przy kontakcie telefonicznym zawsze stosuj metodę ograniczonego zaufania!

Q Securities S.A. z siedzibą w Warszawie, ul. Marszałkowska 142, 00-061 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000446527, NIP: 1080014541, REGON: 146488304 Kapitał zakładowy: 951.570,00 zł (opłacony w całości)

- **Czym jest Vishing?** Vishing to pozyskanie poufnych informacji z wykorzystaniem rozmowy telefonicznej. Przestępcy podszywają się pod znane osoby lub instytucje i w ten sposób zdobywają zaufanie rozmówcy. Często, pod pretekstem konieczności dodatkowej autoryzacji, aktualizacji danych, udostępnienia nowych funkcjonalności, czy awarii systemów pytają o dane osobowe, dostępowe lub namawiają do zainstalowania aplikacji (np. AnyDesk) uzyskując w ten sposób dostęp do telefonu lub komputera, które wykorzystują następnie do kradzieży danych lub pieniędzy. Jest to inny rodzaj phishingu, bo nazwa tego oszustwa to kombinacja słów „voice phishing", czyli phishing głosowy.

- **Jak uchronić się od Vishingu?** Nigdy nie podawaj osobie, która dzwoni swojego loginu i hasła do bankowości oraz numerów kart, bo to są dane, które powinny być znane tylko Tobie. Jeżeli nie masz pewności, czy osoba, która dzwoni, jest pracownikiem Q Securities, to zerwij połączenie. Nie akceptuj żadnej alternatywy kontaktu (e-mail, SMS). W tej sposób oszuści będą próbowali wysłać Ci link lub załącznik, który zainfekuje Twoje urządzenie.

Q Securities

Zasady bezpiecznego korzystania z sieci:

I. **Zastanów się, zanim klikniesz lub odpowiesz**
   - ✓ Nie klikaj w linki i załączniki w wiadomościach e-mail lub SMS od nieznanych nadawców,
   - ✓ Uważnie czytaj SMS-y i powiadomienia, które od Nas dostajesz.

II. **Chroń swoje hasła**
   - ✓ Nigdy nie udostępniaj swojego loginu, hasła i PIN-u osobom trzecim
   - ✓ Pobieraj aplikacje tylko z oficjalnych sklepów - Google Play lub App Store
   - ✓ Przypominamy, że hasła warto okresowo zmieniać (np. raz w miesiącu). Pamiętaj, że w ten sposób dodatkowo podnosisz poziom bezpieczeństwa! Hasło powinno spełniać następujące zasady tj. posiadać minimum 8 i maksymalnie 20 znaków, małe i duże litery (łącznie z polskimi znakami), cyfry i znaki specjalne, zawierać przynajmniej jedną literę i cyfrę.

III. **Bezpieczne logowanie**
   - ✓ Loguj się do panelu klienta Q Securities zawsze bezpośrednio ze strony internetowej www.qsecurities.com a następnie wejdź w zakładkę *Panel Klienta.* Nie używaj w tym celu wyszukiwarek internetowych ponieważ znalezione odpowiedzi mogą odsyłać do nieprawidłowych lub fałszywych stron
   - ✓ Upewnij się, że znalazłeś się na właściwej stronie tj. sprawdź, czy w polu adresu strony w przeglądarce wyświetla się: https://system.qsecurities.pl/front/login/klient,
   - ✓ Upewnij się, że w przeglądarce wyłączona jest funkcja zapamiętywania haseł internetowych. Nie powierzaj również swoich danych logowania żadnym aplikacjom do zarządzania hasłami
   - ✓ Sprawdź, czy w oknie przeglądarki przed adresem strony pojawił się znak kłódki – to oznacza, że połączenie jest szyfrowane, czyli wszystkie dane wymieniane między Twoją przeglądarką, a serwerami Q Securities są zaszyfrowane

IV. **Certyfikat bezpieczeństwa**
   - ✓ Certyfikat strony internetowej to potwierdzenie, że faktycznie połączyłeś się ze stroną Q Securities
   - ✓ Certyfikat bezpieczeństwa sprawdzisz klikając w symbol zamkniętej kłódki po lewej stronie na pasku adresowym przeglądarki. Po kliknięciu w kłódkę zobaczysz opis certyfikatu bezpieczeństwa - poszukaj w nim sekcji tzw. odcisku (ang. *fingerprint*). Poprawna wartość dla Naszego certyfikatu to: SHA-256
     D1 A8 30 7F 3B 5B 8E CD DE CB 74 E6 EA 0B 06 CC F5 B2 CD 5C EE 77 C5 36 7D 25 2F 1F 16 D1 1D F3

V. **Chroń swój sprzęt i swoje informacje**
   - ✓ Stosuj silne hasła, używaj biometrii, Face ID i mobilnej autoryzacji
   - ✓ Zainstaluj program antywirusowy, a urządzenia, na których się logujesz, dodaj do zaufanych.
   - ✓ Zabezpiecz sprzęty hasłem, biometrią lub PIN-em

VI. **Zachowaj dyskrecję w sieci i publicznie**
   - ✓ Gdy przesyłasz do Nas swoje dane np. e-mailem, zabezpiecz je hasłem, które wyślesz SMS-em
   - ✓ Zmień ustawienia prywatności w mediach społecznościowych, treści publikuj tylko znajomym

VII. **Jeśli coś podejrzewasz — zgłoś to!**
   - ✓ Jeśli coś Cię niepokoi w informacjach otrzymanych od pracownika Q Securities - zadzwoń do Nas i poinformuj Nas o tym pod numerem telefonu: + 48 22 417 44 00.