Najważniejsze zasady bezpieczeństwa Twojego konta w STS

1
Nie podawaj nikomu swojego hasła

Hasło jest Twoją własnością i nikomu go nie ujawniaj. Nie wysyłaj haseł mailem lub SMS-em. Hasło należy do Ciebie i żadna odpowiedzialna organizacja nie będzie prosić o jego podanie. Jeżeli ktoś prosi o podanie hasła w wiadomości e-mail, SMS czy przez telefon to na pewno jest próba jego wyłudzenia.

2
Nie podawaj nikomu swoich informacji osobistych w całości

Jeżeli ktoś zadzwoni do Ciebie i poprosi o podanie numeru PESEL w celu weryfikacji, **nie podawaj go**. Nie kontynuuj rozmowy, jeżeli nie spodziewasz się jej.

Jeżeli spodziewasz się kontaktu, Ty poproś osobę dzwoniącą o podanie części PESELU albo innej informacji osobistej (możesz poprosić o kilka informacji), aby się uwiarygodniła i dopiero wtedy kontynuuj rozmowę.

3
Stosuj zdania jako hasło

Stosuj normalne, ale nieszablonowe, zdania złożone z kilku wyrazów (passphrase) np.: „10 Tygrysów w 7 klapkach!" (hint: spacja to również znak w haśle).

4
Nie używaj tego samego hasła w wielu miejscach

Hasło do Twojego konta w STS musi być inne niż do pozostałych systemów. Pamiętaj, że na Twoim koncie znajdują się Twoje pieniądze. Jeżeli Twoje hasło wycieknie z innego systemu, a logujesz się nim także do STS, to ktoś może zalogować się do Twojego konta.

5
Komplikuj zapis hasła

Zamiast litery „A” i „a” stosuj znak „@” (małpa); zamiast „E” i „e” stosuj cyfrę 3; zamiast litery „l” i „i” stosuj cyfrę 1. Wykorzystuj wielkie i małe litery oraz cyfry i znaki specjalne np.: „#,%,^,&”.

6
Zmieniaj cyklicznie hasło

Zmieniaj hasło cyklicznie co 30 dni. To dobra praktyka.

7
Sprawdź, czy Twoje dane wyciekły

Na stronie https://haveibeenpwned.com/ możesz sprawdzić, czy Twoje dane wyciekły. Jeżeli okaże się, że tak, zmień jak najszybciej hasło do swojego konta na nowe, nigdy wcześniej nieużywane.

8
Zmień hasło natychmiast po wykrytym naruszeniu

Jeżeli dowiesz się o wycieku haseł, np.: z prasy, radia, telewizji, od innej osoby lub podejrzewasz, że mogło do niego dojść, zmień hasła do wszystkich systemów, których dotyczy wyciek.

9
Nie zapisuj haseł w przeglądarce internetowej

Nigdy nie zapamiętuj (zapisuj) haseł w przeglądarce internetowej. Hasła nie są szyfrowane i łatwo je odczytać, nawet niedoświadczonej osobie.

10
Korzystaj z konta tylko na własnych urządzeniach

Aby grać w STS, używaj komputera osobistego i własnej komórki. Nie korzystaj z urządzeń współdzielonych albo należących do innych osób.

Jak nie dać się oszukać.
Phishing

1
Zweryfikuj adres nadawcy wiadomości albo adres strony

Sprawdź, czy w nazwie nadawcy nie ma błędów oraz czy domena pasuje do osoby lub firmy, która napisała do Ciebie wiadomość, np. lod@sts.pl (zwróć uwagę, że w „lod" zamiast małej litery „i" jest mała litera „L")

Łatwo można pomylić:

- i = l (pierwsza litera to "i" a druga litera to "el"),
- m = rn (pierwsza litera to "m" a druga, to dwie litery "er" i "en"),
- l = l (pierwsza litera to wielkie "i" a druga to małe "el"),
- g = q (pierwsza litera do "gie" a druga litera to "ku").

2
Zwróć uwagę na błędy gramatyczne, stylistyczne, ortograficzne w treści

Oszuści często nie dbają o zasady poprawnej interpunkcji, gramatyki czy stylistyki. W ich wiadomościach jest bardzo dużo błędów, które zauważysz, gdy wczytasz się w ich treść. Zdarza się, że od razu widać brak kropek i przecinków oraz rzucają się w oczy zdania rozpoczynające się z małej litery – to oznaki oszustwa.

3
Oddziaływanie na uczucia

W fałszywych wiadomościach oszust często posługuje się treścią, która oddziałuje na Twoje uczucia (wywołuje poczucie strachu, ekscytacji, ciekawości) np.: powiadomienia o wygraniu konkursu, losu na loterii, zawieszeniu konta bankowego, powiadomienia odnoszące się do zaległych płatności lub powiadomienia o przekierowaniu przesyłki.

4
Fałszywe (szkodliwe) odnośniki (linki, hiperłącza)

W wiadomościach phisingowych często są odnośniki, które po kliknięciu przekierowują do fałszywej strony internetowej. Zalecaną praktyką jest najechanie kursorem myszki na odnośnik, aby sprawdzić co się „kryje" w odnośniku. Gdy najedziesz kursorem myszki na odnośnik, zobaczysz adres (najczęściej w postaci dymku, wyskakującego okienka), do którego kieruje ten odnośnik.

Przykład fałszywego odnośnika: www.qooqle.com - czy widzisz, że litera „g" to tak naprawdę litera „q"? Ta witryna istniała naprawdę i była oznaczona jako rozprzestrzeniająca szkodliwe oprogramowanie.

5
Załączniki w mailu

Często cyberprzestępcy dodają do wiadomości e-mail załączniki o tytułach „Zaległa faktura.pdf.zip", „Zdjecie.pdf.exe", itd., które mają Cię zachęcić do jej otwarcia. Rozszerzenia zip, rar, exe, gz, arj, tgz są charakterystyczne dla folderów, w których najczęściej jest złośliwe oprogramowanie. Oszust może nim zainfekować Twoje urządzenie lub nawet pozyskać z niego wszystkie Twoje dane. Oszuści często używają podwójnych rozszerzeń pliku, aby Cię zmylić.

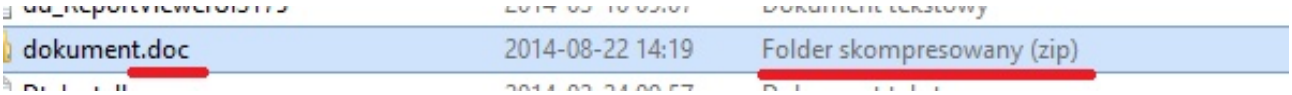
Pamiętaj, aby zawsze zwracać uwagę na rozszerzenie, które jest ostatnim członem w nazwie pliku, np. PRZYKŁAD.pdf.zip. To nie jest dokument PDF, tylko archiwum skompresowanych plików, które po rozpakowaniu i uruchomieniu mogą np.: zaszyfrować Twój dysk.

6
Ukrywanie rozszerzeń w systemie Windows może wprowadzić w błąd

Warto wspomnieć o pewnym mechanizmie w systemach Windows, który ma ułatwiać pracę, ale czasami jest wykorzystywany w celu zmylenia użytkownika. Domyślnie system Windows ukrywa

najpopularniejsze rozszerzenia z nazw plików i np. mając plik „dokument.doc", system Windows wyświetla go jako „dokument". Jednak w przypadku, kiedy mamy plik „dokument.doc.zip", to system ukryje rozszerzenie („zip") i pokaże „dokument.doc", co na pierwszy rzut oka nie wydaje się podejrzane.

Należy pamiętać o tej właściwości systemu i w przypadku posiadania wśród wielu plików bez rozszerzenia, kilku z rozszerzeniem, wzmóc czujność.



7
Monitorowanie Twoich danych przez BIK

Możesz skorzystać z płatnej usługi oferowanej przez Biuro Informacji Kredytowej pod adresem

https://www.bik.pl/

Dzięki temu otrzymasz powiadomienie SMS o próbie złożenia wniosku kredytowego na Twoje dane.

8
Monitorowanie Twoich danych przez KRD

Możesz skorzystać z płatnej usługi oferowanej przez Krajowy Rejestr Długów pod adresem

https://chronpesel.pl/

Dzięki temu otrzymasz powiadomienie SMS o próbie wykorzystania Twojego numeru PESEL.

9
Jeśli masz chwilę, przeczytaj:

https://akademia.nask.pl/blog/2/phishing--czym-jest-i-jak-nie-dac-sie-zlowic-oszustom_i24.html

https://akademia.nask.pl/blog/2/hasla-i-bezpieczenstwo-danych_i22.html

https://www.gov.pl/web/baza-wiedzy/najpopularniejsze-oszustwo-internetowe--phishing