UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

BĄDŹMY BEZPIECZNI W SIECI!

Nie daj się oszukać! Przeczytaj wskazówki i podziel się nimi ze znajomymi

1. Nie udostępniaj nieznanym osobom swoich danych ani dokumentów tożsamości
Oszuści często umieszczają w Internecie fałszywe ogłoszenia o pracę. Odpowiadasz na ogłoszenie? Nie załączaj skanu swoich dokumentów ani numeru PESEL.

2. Nie musisz nic płacić chcąc zacząć pracować
Nie rób żadnych przelewów, w zamian za otrzymanie pracy lub jej obietnicę. Jeżeli ktoś oferuje Ci pracę polegającą na przesyłaniu pieniędzy z konta na konto, lub proponuje założenie kilku kont bankowych i udostępnienie ich – jest to oszustwo!

3. Nikomu nie udostępniaj danych logowania do banku
Nie podawaj nikomu swojego loginu ani hasła do banku. Nie udostępniaj również numeru PESEL, loginu ani hasła do profilu zaufanego.

4. Nie udostępniaj numeru karty płatniczej
Jeżeli ktoś prosi Cię o podanie numeru karty, aby przelać na nią środki to prawdopodobnie jest to oszustwo. Nie podawaj numeru karty ani kodu CVV, który znajduje się na odwrocie karty.

5. Uważaj na promocje lub wyjątkowe okazje
W przypadku gdy znajdziesz lub otrzymasz atrakcyjną ofertę, pamiętaj, aby zachować szczególną ostrożność. Coraz częściej oszuści oferują np. tani wynajem mieszkań. Wymagają jednak przedpłaty lub przesłania skanu dokumentów. W rzeczywistości oferowane przez nich mieszkanie nie istnieje a przekazane dane posłużą celom przestępczym.

6. Nie klikaj w linki z SMS-ów
Pamiętaj, że linki znajdujące się w wiadomościach SMS bardzo często prowadzą do fałszywych stron. Często znajduje się tam złośliwe oprogramowanie lub fałszywy panel płatności. Obie metody oszustwa powodują utratę pieniędzy.

7. Sprawdzaj linki stron
Sprawdzaj adresy stron, na które wchodzisz z otrzymanych wiadomości sms lub e-mail. Często, pomimo tego, że adres wydaje się być poprawny, może on różnić się jednym znakiem. Najbezpieczniej jest samodzielnie wpisać adres strony, na którą chcesz wejść.

8. Weryfikuj informacje
Dokładnie weryfikuj informacje i zachowaj ostrożność. Popularnym w Polsce oszustwem jest przejmowanie źle zabezpieczonych kont w mediach społecznościowych i wysyłanie do znajomych próśb o przelew.

Jeżeli otrzymałeś wiadomość z podejrzaną treścią, prześlij ją na adres cert@cert.pl

KNF CSIRT

Więcej ostrzeżeń znajdziesz na naszym Twitterze:
https://twitter.com/CSIRT_KNF

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Будьмо безпечні в інтернеті!

Не дайте себе обдурити! Прочитайте ці рекомендації і поділіться ними зі знайомими.

1. Не передавайте незнайомим людям своїх даних чи документів, що посвідчують особу
Шахраї часто розміщують в інтернеті неправдиві оголошення про роботу. Ви відповідаєте на оголошення? Не додавайте сканів своїх документів чи номера PESEL.

2. Не треба нічого платити перед початком роботи
Не робіть жодних грошових переказів взамін за отримання роботи або обіцянку щодо отримання роботи. Якщо хтось пропонує вам роботу, яка полягає в пересиланні грошей з рахунку на рахунок, або пропонує відкриття кількох банківських рахунків і вимагає надати доступ до них – це шахрайство!

3. Не давайте нікому даних для авторизації в банку
Не давайте нікому свого логіна і пароля для авторизації в банку. Це стосується також номера PESEL, логіна та пароля до довіреного профілю.

4. Не давайте нікому номера платіжної картки
Якщо хтось просить вас дати номер картки, щоб перерахувати на неї кошти, є велика ймовірність, що це шахрайство. Не давайте номера картки і коду CVV, розташованого на зворотному боці картки.

5. Будьте обережні, коли пропонуються знижки чи вигідні акції
Якщо ви знайдете або отримаєте привабливу пропозицію, пам'ятайте, що слід зберігати особливу обережність. Щораз частіше шахраї пропонують, наприклад, дешеву оренду квартир. Однак при цьому вимагають внести передплату або надіслати скан документів. У дійсності запропонована ними квартира не існує, а передані дані використовуватимуться зі злочинною метою.

6. Не клікайте в посилання з SMS-повідомлень
Пам'ятайте, що посилання, які знаходяться в SMS-повідомленнях, дуже часто ведуть до підроблених сайтів. Там часто розміщене шкідливе програмне забезпечення або підроблена панель для сплати платежів. Обидва методи шахрайства призведуть до того, що ви втратите гроші.

7. Перевіряйте адреси сайтів
Перевіряйте адреси сайтів, на які ви заходите з отриманих SMS-повідомлень або електронних листів. Часто, хоча адреса здається правильною, вона може відрізнятися одним символом. Найбезпечніше самостійно вписати адресу сайта, на який ви хочете зайти.

8. Перевіряйте інформацію
Ретельно перевіряйте інформацію і будьте обережними. Популярним у Польщі шахрайством є викрадення погано захищених профілів та сторінок у соціальних мережах і надсилання знайомим прохань зробити грошовий переказ.

Якщо ви отримали інформацію з підозрілим змістом, надішліть її на адресу cert@cert.pl

KNF CSIRT

Більше інформації щодо безпеки можна знайти на нашій сторінці у Twitter:
https://twitter.com/CSIRT_KNF