Құрметті салымшылар!

Қазіргі заманда алаяқтар жеке және қаржылық деректерге қол жеткізу үшін телефон қоңырауларын, SMS, электрондық поштаны және әлеуметтік желілерді пайдаланады. Осы деректерді қорғау сіздің ақпаратыңызды сақтауға және қаржылық шығындарды болдырмауға көмектеседі.

Төменде тәуекелдерді азайтуға және алаяқтықты болдырмауға көмектесетін ұсынымдар берілген.

1. Неге назар аудару керек

Телефон қоңыраулары:

- Зейнетақы қорының, банктердің немесе мемлекеттік органдардың атынан деп кодтарды, парольдерді немесе карта деректемелерін хабарлауды өтінген қоңыраулар.
- «Операцияны шұғыл растау қажет», «Сіздің шотыңыз бұғатталған» сияқты шұғыл әрекет ету сезімін қалыптастыру.

SMS және мессенджерлер:

- Жеке деректерді енгізу үшін жалған сайттарға сілтемелері бар хабарламалар.
- «Ақшаны күдікті есептен шығару» немесе «ерекше белсенділік» туралы хабарламалар.

Электрондық пошта:

- Қызметтерді төлеуді, тіркемелерді жүктеуді немесе құжаттарды тексеруді сұраған хаттар.
- Сілтемелер алаяқтық сайттарға әкелуі мүмкін.

Әлеуметтік желілер:

- Таныстардың немесе ресми тұлғалардың жалған аккаунттары.
- Қаражатты аудару немесе құпия ақпаратты ұсыну туралы сұраулар.

2. Қандай деректерді беруге болмайды

Қандай жағдай болмасын мыналарды хабарламаңыз:

- SMS, push-хабарламалардан немесе қосымшалардан растау кодтары.
- Банк карталарының толық деректері: нөмірі, қолданылу мерзімі, CVV/CVC.
- Жеке немесе жұмыс аккаунттарынан логиндер мен парольдер.
- QR кодтары және бір рет қолданылатын токендер.
- Дербес деректер, табыстар туралы ақпарат және басқа да құпия ақпарат.

3. Практикалық ұсынымдар

1. **Сұрау салу көзін тексеріңіз.** Егер қоңырау немесе хат күдік тудырса, ұйыммен ресми байланыс арқылы тікелей байланысқа шығыңыз.
2. **Күмәнді сілтемелер арқылы өтпеңіз.** Браузерде сайт мекенжайын қолмен енгізіңіз.
3. **Қауіпсіз байланыс арналарын пайдаланыңыз.** Құпия деректерді жеке мессенджерлер немесе әлеуметтік желілер арқылы бермеңіз.
4. **Парольдерді жаңартып отырыңыз және күрделі комбинацияларды пайдаланыңыз.** Түрлі сервистер үшін бірдей парольдерді пайдаланбаңыз.
5. **БҚ мен антивирустардың жаңартылуын қадағалап отырыңыз.** Өзекті нұсқалар зиянды файлдардың ену қаупін төмендетеді.
6. **Белгісіз құрылғыларды қоспаңыз.** USB-флешкалар мен сыртқы дискілерде зиянды БҚ болуы мүмкін.
7. **Тіркемелер мен файлдармен абай болыңыз.** Дереккөзді растап болғаннан кейін ғана оларды ашыңыз.

4. Күдікті оқиғалар кезіндегі іс-қимылдар

Егер сіз күдікті қоңырау, хат немесе хабар алсаңыз:

- Белгісіз адаммен сөйлесуді тоқтатыңыз.
- Деректерді енгізбеңіз және тіркемелерді ашпаңыз.
- Болған жағдай туралы қолдау қызметіне хабарлаңыз.
- Қажет болған жағдайда карталарды немесе онлайн-сервистерге кіруді бұғаттаңыз.

Ақпараттық қауіпсіздіктің қарапайым ережелерін сақтау жеке деректерді қорғауға, қаржылық шығындарды болдырмауға және беделді сақтауға көмектеседі. Қорғаудың негізгі шаралары – дереккөздерді жылдам тексеру, ақпаратты беру кезіндегі сақтық және байланыстың қауіпсіз арналарын пайдалану.

Уважаемые вкладчики!

В современном мире мошенники используют телефонные звонки, SMS, электронную почту и социальные сети, чтобы получить доступ к личным и финансовым данным. Защита этих данных помогает сохранить вашу информацию и предотвратить финансовые потери.
Ниже представлены рекомендации, которые помогут снизить риски и избежать мошенничества.

1. На что обращать внимание

Телефонные звонки:

- Звонки якобы от имени пенсионного фонда, банков или государственных органов с просьбой сообщить коды, пароли или реквизиты карт.
- Создание чувства срочности: «Необходимо срочно подтвердить операцию», «Ваш счет заблокирован».

SMS и мессенджеры:

- Сообщения с ссылками на поддельные сайты для ввода личных данных.
- Уведомления о «подозрительных списаниях» или «необычной активности».

Электронная почта:

- Письма с просьбой оплатить услуги, скачать вложения или проверить документы.
- Ссылки могут вести на мошеннические сайты.

Социальные сети:

- Поддельные аккаунты знакомых или официальных лиц.
- Запросы о переводе средств или предоставлении конфиденциальной информации.

2. Какие данные нельзя передавать

Ни при каких обстоятельствах не сообщайте:

- Коды подтверждения из SMS, push-уведомлений или приложений.
- Полные данные банковских карт: номер, срок действия, CVV/CVC.
- Логины и пароли от личных или рабочих аккаунтов.
- QR-коды и одноразовые токены.
- Персональные данные, информацию о доходах и другую конфиденциальную информацию.

3. Практические рекомендации

1. **Проверяйте источник запроса.** Если звонок или письмо вызывает подозрение, свяжитесь с организацией напрямую через официальные контакты.
2. **Не переходите по сомнительным ссылкам.** Введите адрес сайта вручную в браузере.
3. **Используйте безопасные каналы связи.** Не передавайте конфиденциальные данные через личные мессенджеры или социальные сети.
4. **Обновляйте пароли и используйте сложные комбинации.** Не используйте одинаковые пароли для разных сервисов.
5. **Следите за обновлениями ПО и антивирусов.** Актуальные версии снижают риск заражения вредоносными файлами.
6. **Не подключайте неизвестные устройства.** USB-флешки и внешние диски могут содержать вредоносное ПО.
7. **Будьте осторожны с вложениями и файлами.** Открывайте их только после подтверждения источника.

4. Действия при подозрительных событиях

Если вы получили подозрительный звонок, письмо или сообщение:

- Прекратите общение с неизвестным лицом.
- Не вводите данные и не открывайте вложения.
- Сообщите о ситуации в службу поддержки.
- При необходимости заблокируйте карты или доступ к онлайн-сервисам.

Соблюдение простых правил информационной безопасности помогает защитить личные данные, избежать финансовых потерь и сохранить репутацию. Быстрая проверка источников, осторожность при передаче информации и использование безопасных каналов связи ключевые меры защиты.