

Осторожно: мошенники! Ваша безопасность - в ваших руках!

Рассмотрим несколько реальных случаев мошенничества, актуальных на сегодняшний день, а также простые правила поведения, которые помогут обезопасить ваши деньги.

Пример №1. Лжепокупатели звонят своим жертвам, заявляя, что хотят купить товар и готовы внести предоплату. При этом мошенники, представляясь бухгалтерами или директорами фирм, просят указать ряд реквизитов: ИИН, номер телефона, к которому привязана карта, номер банковской карты, номер текущего или сберегательного счета. Когда продавец указывает реквизиты, они просят продиктовать код из SMS-сообщения, отправленного на номер жертвы якобы для активации перевода денег. После получения кода мошенники меняют номер телефона в интернет-банкинге клиента и выводят деньги со счетов.

Особенно это актуально при продажах на торговых интернет-площадках, где никто не контролирует взаимоотношения продавца и покупателя. Поэтому при совершении любых операций на таких ресурсах необходимо помнить несколько основных правил:

- Ни при каких обстоятельствах не отправляйте незнакомым людям ваши персональные данные, включая копии документов, удостоверяющих личность;
- Никогда не передавайте и не публикуйте (в том числе в социальных сетях) реквизиты платежной карты: 16-значный номер, имя держателя, срок действия, CVV/CVC-код (трехзначный номер на тыльной стороне карты);
- Никому не сообщайте SMS-коды для авторизации и подтверждения операций, в том числе сотрудникам банка;
- Не передавайте свои банковские карты третьим лицам (даже родственникам), в том числе для проведения платежей в кафе и ресторанах;
- В случае утери карты сразу же блокируйте ее и приостанавливайте все операции, позвонив на горячую линию банка, также желательно посетить отделение банка в кратчайшие сроки с целью блокировки счетов;
- Сотрудники банков никогда не звонят первыми клиенту с требованием предоставить данные по карте либо полученные SMS. Любое общение по данным вопросам инициируется исключительно клиентом;
- Если вы совершаете платежи и покупки с использованием банковской карты через Интернет, не открывайте подозрительную почту и не переходите по неизвестным ссылкам. В них может содержаться вирус, способный дистанционно передать мошенникам информацию с вашего компьютера;
- Подключите за символическую ежемесячную плату услугу мобильного банка, чтобы на ваш мобильный телефон приходила информация по всем изменениям счета и совершенным транзакциям. Таким образом, вы сможете



оперативно отследить подозрительные операции по вашей карте.

Пример №2. Вы потеряли или, что хуже, у вас украли мобильный телефон. Мошенники могут снять деньги либо совершить оплату с ваших счетов путем регистрации в интернет-банкинге по номеру украденного телефона или попросту зайти в уже установленный мобильный банкинг или мобильное приложение.

В первую очередь необходимо заблокировать свои счета, обратившись в CALL-центр банка или ближайшее отделение банка, а также через Интернет-банкинг.

Параллельно необходимо заблокировать номер украденного телефона через мобильного оператора.

Пример №3. Потенциальной жертве звонят якобы сотрудники банка, заявляя, что обнаружили подозрительные операции по банковской карте и с целью их предотвращения просят указать ряд реквизитов: ИИН, номер телефона, к которому привязана карта, номер банковской карты, номер текущего или сберегательного счета. При этом они оказывают постоянное психологическое давление, говоря, что в случае, если не предоставить им данные, все деньги будут потеряны моментально.

Что же делать в такой ситуации? Повесьте трубку и позвоните в банк, который вас обслуживает, для уточнения информации с мобильного телефона, а еще лучше посетите ближайшее отделение вашего банка и напишите официальное заявление о попытках совершения атак на ваши счета. Ни в коем случае не продолжайте диалог со злоумышленниками и не сообщайте им никакую информацию.

Существует регламент действий сотрудников банков, в соответствии с которым сотрудники банков никогда не звонят клиенту первыми и не выставляют требования предоставить данные по карте, личные данные либо полученные SMS.

Любое общение по данным вопросам инициируется исключительно клиентом.

Пример №4. Мошенники создали клон популярного интернет-магазина, сайта банка либо социальной сети с целью получения реквизитов ваших платежных карт, так называемый фишинговый сайт. Ссылки на него распространяются через имеющуюся базу почтовых адресов, в числе которых может оказаться и ваш адрес.

Чтобы не попасть на уловки интернет-мошенников, помните несколько правил:

- нигде не указывайте ваши персональные данные;
- обращайте внимание на оформление сайта;
- проверяйте правильность ссылки в адресной строке;
- пользуйтесь защищенным соединением https;
- фильтруйте подозрительные письма;
- не пользуйтесь открытыми точками доступа wi-fi для входа в банковские аккаунты;
- обращайте внимание на форму оплаты. В надежных интернет-магазинах она открывается в новом окне и имеет верификацию одной из платежных систем (VISA, Mastercard).

Пример №5. Лжепродавцы размещают на торговых или информационных площадках «горящее» объявление о продаже недвижимости, либо транспортных средств по заниженной цене. При этом мошенники, представляясь работником иностранной фирмы, рассказывают о том, что срочно уехали из Казахстана по работе и просят отправить денежные средства посредством быстрых переводов на имя своего родственника для подтверждения платежеспособности. Когда покупатель осуществляет перевод, они просят продиктовать реквизиты перевода якобы для его проверки. После получения реквизитов мошенники осуществляют выплату перевода на свое имя.

Помните, что любая сделка должна быть совершена и зарегистрирована официально и в правовом поле. Даже в случае предоплаты, создается отдельный документ (расписка) о ее получении.

Соблюдение этих простых, но эффективных правил позволит уберечь ваши средства от коварных мошенников. Кстати, наиболее актуальны эти правила для пожилых людей. Обязательно расскажите о них своим родным и близким, чтобы они никогда не попались на удочку мошенников. И всегда помните, что бесплатный сыр бывает только в мышеловке! Берегите свои персональные данные, в случае обнаружения их пропажи немедленно блокируйте счета, номера телефонов, привязанные к ним, и обращайтесь в правоохранительные органы.

Fingramota.kz

Консультативный прогноз погоды на июль 2022 года



В течение первой декады месяца на большей части Казахстана, с влиянием циклонической деятельности и прохождением атмосферных фронтов, ожидается неустойчивый характер погоды.

Пройдут дожди, временами сильные: в западных регионах Казахстана в начале месяца, на остальной территории страны - в середине первой декады июля.

Дождливая и пасмурная погода будет сопровождаться грозами, градом, шквалом и усилением ветра с порывами

до 15-25 м/с. В этот период с вторжением холодных воздушных масс из районов Северных морей в северной половине страны температурный фон ночью составит +5+13°C, днем ожидается понижение температуры воздуха от +18+28°C до +12+17°C, в южной половине республики - спад жары прогнозируется ночью от +20+25°C до +12+20°C, днем от +30+38°C до +23+30°C.

В конце первой и в начале второй декады июля вновь вернутся жаркие летние дни. Дневные температуры воздуха будут повышаться:

- в юго-западной половине страны до +30+40°C;
- на севере, центре и востоке до +25+33°C.

Пресс-служба РГП «Казгидромет»

ТОО «Спектр-КР» объявляет о проведении общественных слушаний по проекту Раздел «Охрана окружающей среды» к плану разведки твердых полезных ископаемых «Расположен в пределах 3 блоков М-42-12-(10д-5б-14,15), М-42-12-(10е-5а-11) в Акмолинской области (лицензия №673-ЕЛ от «30» июня 2020 года)» и проектов НДВ, ПЭК, ПУО.

Общественные слушания состоятся 12 августа 2022 года в 15:00. По адресу: Акмолинская область, Новосельский с.о, с. Каратобинское, ул. Ак-Жайык 1

В случае продления карантинных мер, общественные слушания будут проведены в режиме онлайн на платформе Zoom.

Для участия в слушаниях необходимо пройти по ссылке:
<https://us04web.zoom.us/j/72559953000?pwd=V>

ЕроalpubJyenc0eUJ2UXc3bEzWQT09
Идентификатор конференции: 248 741 0037
Пароль: jks7uG
Заказчик: ТОО «Спектр-КР», тел 8 (716-45) 7-11-72

Разработчик проекта ОВОС: Фирма «КазЭкоПроект» ИП Борщенко С.В., конт. тел: 8(7162) 52-52-60

С материалами общественных слушаний можно ознакомиться на сайте esorogtal.kz.

Дополнительную информацию по проекту можно запросить по тел. 8(716-2)52-52-60, kazecoproect2012@mail.ru

Замечания и предложения принимает ГУ «Управление природных ресурсов и регулирования природопользования Акмолинской области» по адресам: expreso@mail.ru и г. Кокшетау, ул. Абая, 89.

На основании закона РК от 19.02.2001 года № 143-III «О зерне» в целях своевременной подготовки материально-технической базы к приемке и хранению зерна урожая 2022 года ТОО «Жер-Ана» уведомляет о том, что с 20.06.2022 года элеватор начинает ежегодную подготовку МТБ. Прием и отгрузка зерна будет производиться после окончания МТБ с 08.08.2022 года.

Тлектес -3

ИЗГОТОВЛЕНИЕ и Установка
матллопластиковых
ОКОН, ДВЕРЕЙ, ВИТРАЖЕЙ,
БАЛКОНОВ,

пластиковых откосов из профиля
производства Германии Funke.

ГАРАНТИЯ КАЧЕСТВА!

Обращаться: 8-701-342-77-72,
8707-84-55-338, 8777-370-70-01



Вестник Шортанды

районная общественно-политическая газета

Собственник газеты: ТОО «Редакция газет «Жаршы» и «Вестник» Шортандинского района

Регистрация: МИК РК №17576-Г от 06.03.2019

Главный редактор: Гульзияш Кабдешова

Редактор газеты: Инна Минасян

Бухгалтер: Наталья Миханчик

Адрес редакции: 021600, п.Шортанды, ул.Мира, 11

Тел. 2-12-95, 7-90-33

Электронный адрес: gazetavestyl@mail.ru

Газета выходит по четвергам на русском языке.

Отпечатано ИП Дунасарова А.Д. г. Нур-Султан, ул. Жубанова, 24/1.

Мнение авторов публикации не обязательно отражает точку зрения редакции. PR- материал на коммерческой основе.

Ответственность за содержание рекламы и объявлений несет рекламодатель.

Тираж 204 экз. Заказ: 130