ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Презентация в рамках реализации Стратегии повышения финансовой грамотности в РФ

ФИНАНСОВОЕ МОШЕННИЧЕСТВО – это совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

-с банковскими картами

-кибермошенничество

Виды финансового мошенничества

-на финансовых рынках

-финансовые пирамиды

ПРИЗНАКИ ФИНАНСОВОГО МОШЕННИЧЕСТВА

- **Гарантии высокого дохода (свыше 20%)**
- **Агрессивная и навязчивая реклама**
- **Предварительный взнос организаторам помимо вложений**
- **Просьба приводить новых клиентов за щедрые гонорары от их взноса (20-30%)**
- **Оффшорная регистрация компании. Все легальные финансовые конторы сейчас имеют юридическую прописку в России**
- **Страхование средств в малоизвестной компании. Может оказаться, что риск невозврата ваших сбережений застраховать «забыли»**

Мошенничество с банковскими картами

Кража карты	**Происходит, как правило, вблизи банкоматов. ПИН-код мошенник может подсмотреть у банкомата«через плечо» или при помощи миниатюрной видеокамеры**
Скимминг (от английского «to skim» — бегло прочитывать, скользить)	**Считывание информации с магнитной полосы карты с помощью специального технического устройства или скиммера, который можно установить на банкомат. Получив данные карты, ее можно скопировать и вывести все деньги.**
Траппинг или «Ливанская петля»	**В картридер банкомата вставляется кусок фотопленки (чаще пластик), надрезанный таким образом, что карта, попадая в прорезь, не возвращается обратно владельцу, а попадает в некий конверт, который впоследствии извлекается мошенником. В момент, когда карта попадает в ловушку, злоумышленник оказывается рядом с потерпевшим и предлагает ему ввести повторно ПИН-код, мотивируя это тем, что с ним накануне произошла подобная ситуация и это помогло вернуть карту. После «неуспешных» вводов ПИН-кода пластик, естественно, не возвращается, и мошенник советует обратиться в банк. Когда потерпевший уходит, конверт вместе с картой извлекается мошенником из банкомата. В итоге у преступника не только оказывается карточка потерпевшего, но и информация о ее ПИН-коде.**
Фишинг (англ. «fishing» — «рыбная ловля»)	**Выуживание контрольной информации и персональных данных владельца карты от самого владельца карты. Этот вид мошенничества стал массово распространяться именно сейчас, поскольку для дистанционных операций через интернет сама карта теперь уже не нужна.**

ФИНАНСОВЫЕ ПИРАМИДЫ - это мошенническая схема извлечения прибыли, за основу которой взято постоянное привлечение новых вкладчиков, а не инвестирование в различные доходные активы. Основным инструментом деятельности подобного механизма является выпуск ценных бумаг, не обладающих на самом деле заявленной ценностью.

Мошенничество на финансовых рынках побуждает инвесторов принимать решения о покупке или продаже на основе ложной информации, часто приводящей к убыткам, в нарушение законодательства о ценных бумагах.

Чтобы не стать жертвой мошенничества на фондовом рынке, рекомендуется внимательно изучать компании, акции и другие ценные бумаги, прежде чем инвестировать, проверять лицензии и сертификаты, не доверять подозрительным онлайн-ресурсам и общаться только с надежными и проверенными контактами.

СПРАВОЧНИК участников финансового рынка размещен на сайте ЦБ РФ https://cbr.ru/

Как НЕ НАДО делать

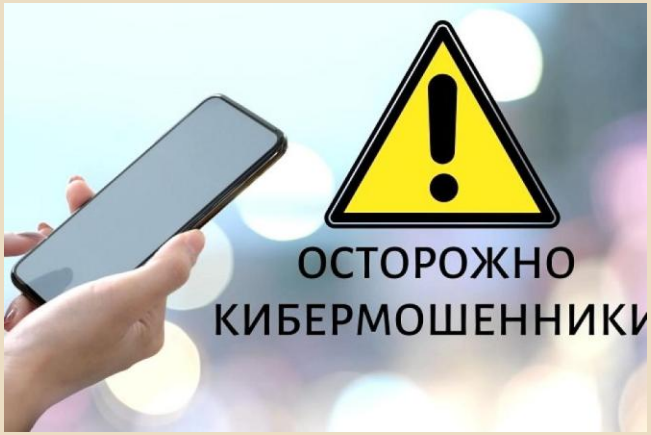
-Нельзя вкладывать в ценные бумаги все, что у вас есть
-Не действуйте на авось — пройдите обучение
-Не поддавайтесь эмоциям
-Не складывайте все яйца в одну корзину
-Не верьте обещаниям зарабатывать 500% в день

КИБЕРМОШЕННИЧЕСТВО - это причинение материального или иного ущерба путём хищения личной информации пользователя (номеров банковских счетов, паспортных данных, кодов, паролей и так далее)

СМС от имени родственника с просьбой перевода денег на неизвестный счет

СМС об ошибочном зачислении средств или с просьбой подтвердить покупку

Звонок якобы от имени банка (просят сообщить личные данные)



Звонок от «следователя Следственного комитета» с сообщением: «Вы – участник уголовного дела!» с требованием о содействии (продажа квартир, оформление кредитов и т.п.)

Вредоносное программное обеспечение

Звонок якобы от сотрудника ЦБ о краже с вашей карты денег

Объявления с QR-кодами, по которым можно якобы получить гарантированную социальную выплату

Популярные схемы обмана в 2023 году

«Темная сеть»
Сейчас злоумышленники могут купить почти любые данные в Даркнете, а именно: ФИО, адрес почты, номера карт, логины онлайн-банков, а также сканы паспортов, СНИЛС, ИНН. Там же продается и вредоносное программное обеспечение, с помощью которого можно легко украсть деньги с банковских счетов.

Новая карта
Доставляют новую пластиковую карту, а через 10-15 минут звонят мошенники и предлагают ее активировать, хотя эту процедуру должен выполнить сам клиент. Таким образом, злоумышленники узнают данные, а потом снимают деньги со счетов.

Звонки из банка, полиции, пенсионного фонда и т.п.
Эта схема обмана одна из самых популярных. Аферисты звонят жертвам под видом банковских сотрудников, полиции или других государственных организаций и пытаются выманить личную информацию клиента. Сначала они усыпляют бдительность человека, а после играют на его доверии.

"Вы - подозреваемый в госизмене"
Участились случаи звонков, когда серьезный голос представляется чином из ФСБ и пугает, что с вашей карты были денежные переводы и вы финансируете зарубежных военных. Даже если и не знали об этом. А значит, являетесь изменщиком родины и вам светит очень серьезный срок с конфискацией всего имущества.

Звонок якобы с Госуслуг
Мошенники звонят, сетуют, что вы давно не заходили на сайт, просят обновить пароли, представляясь сотрудником пенсионного или налоговой. Их цель – получить доступ к учетной записи пользователя со всеми вытекающими последствиями.

ЕСЛИ ВАС ПЫТАЮТСЯ ОБМАНУТЬ

-Будьте уверенными, даже наглыми, не давайте себя запугать. Отнеситесь к этому с юмором и вами никто не сможет манипулировать.
-Не передавайте информацию о себе, карте, финансовом состоянии, не переходите на ссылки и не скачивайте подозрительные приложения.
-Дайте понять, что вы для мошенников бесполезны: вы не клиент этого банка, у вас нет денег, вам не приходят СМС и вам вообще нет 18 лет.
-Будьте неожиданными: спросите «товарища генерала» как он докатился до такого состояния и спросите сколько ему еще сидеть осталось. С понимающими людьми им нет резона разговаривать.
-Тяните время: говорите медленно, тяните слова и предложения в лучших традициях эстонского говора.
-Отвлекайте мошенников от «работы»: попросите их подождать или просто оставьте их «висеть на линии». Можно молчать, «включить дурачка» и делать вид что не понимаете, о чем они говорят.
-Завалите ненужной информацией: расскажите про стерву с работы, и про глупую продавщицу, про сериал и т.п.

-Проигнорируйте и не вступайте в беседу !

ДЕЙСТВИЯ ПОСТРАДАВШЕГО от ФИНАНСОВОГО МОШЕННИЧЕСТВА

Украли карту	• Срочно ее заблокировать по телефону Горячей линии, через Интернет-банк, мобильное приложение или личной явкой в отделение банка
Списали деньги с карты	• Позвоните в банк и заблокируйте карту • Запросите выписку и напишите заявление о несогласии с операцией • Обратитесь в полицию
На Вас оформили кредит (займ)	•**Напишите заявление в полицию** •**Обратитесь в банк или МФО. Напишите заявление о том, что кредит был оформлен на ваше имя мошенническим путем** •**Оставьте претензию и запросите в 2 экземплярах (для полиции и суда) все заверенные копии документов, подтверждающие выдачу займа** •**Подайте иск в суд. Если финансовая организация не согласится с вашей претензией и не спишет задолженность, готовьтесь судиться**
Вложились в финансовую пирамиду и «прогорели»	• Составьте претензию с требованием возврата денег • Если не отдают, обратитесь в полицию • Найдите других жертв мошенников, чтобы действовать сообща

ПРАВИЛА ФИНАНСОВОЙ ГИГИЕНЫ

✓Не сообщайте никому данные своей карты
✓Не вкладывайте деньги в сомнительные предприятия с якобы высокой доходностью
✓Не открывайте письма, файлы, ссылки, пришедшие к вам от неизвестных людей, а также «странные» и неожиданные письма от знакомых
✓Для оплаты товаров и услуг через Интернет рекомендуется завести отдельную дебетовую карту
✓Проверяйте состояние счета после любых операций с картой

Не принимайте поспешных решений

Всегда проверяйте информацию

Если вас обманули – обращайтесь в полицию

СПАСИБО за ВНИМАНИЕ !

Материал подготовлен ФУАМО Кимовский район с использованием Интернет-ресурсов, 2023