TORAIGHYROV UNIVERSITY
НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

Название дисциплины: Безопасность жизнедеятельности

Лекция №13: Основы финансовой безопасности. Основы информационной безопасности

Доктор PhD
Асаинова Диана Кайратовна

Павлодар,
2023 г.

Финансовая безопасность – это про что?

- Пережить временные финансовые трудности (или смягчить их последствия) не снижая уровень жизни и не залезая в долги
- Избежать вложений денег в финансовые пирамиды или высокорискованные инструменты (тем более, взяв на это кредит)
- «Охранять» деньги от мошенников при совершении переводов, платежей и покупки услуг, в том числе, с использованием цифровых сервисов

Цифровизация

- Цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг

Цифровизация – замена физических систем сбора и обработки данных технологическими системами, которые генерируют, передают и обрабатывают цифровой сигнал о своем состоянии

Цифровая среда современного человека:
- диджитализация – настоящий бум жизни онлайн;
- мультиэкранность – Smart-TV, компьютеры, планшеты, смартфоны

«Плюсы» цифровой экономики для потребителей финансовых услуг

- Упрощение финансовых операций, повышение роли электронных и цифровых денег
- Упрощение платежей
- Сокращение затрат
- Удобство доступа
- Гибкость продуктов
- Быстрое информирование клиента
- Возможность получить отчет и проанализировать операции
- Развитие возможностей дистанционной работы
- Внедрение электронного документооборота
- Более открытый и доступный финансовый рынок
- Повышение финансовой грамотности

Риски цифровой экономики для потребителей финансовых услуг

- - риск киберугроз, связанный с проблемой защиты персональных данных;
- «цифровое рабство» – использование данных о человеке для управления его поведением;
- «цифровой разрыв» – разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам, и, как следствие, разрыв в уровне благосостояния людей;
- недостаточная прозрачность цен и условий;
- сложность подачи жалоб;
- риски нерационального поведения на финансовом рынке как следствие доступности операций для неквалифицированных потребителей финансовых услуг;
- риски подверженности новым инструментам мошенничества с использованием цифровых технологий

Финансовая безопасность

- Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений.
- Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условия договоров, отсутствие финансовой дисциплины и - как следствие - неисполнение своих обязательств и неприятная финансовая ситуация.

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

- *Мошенничества с использованием банковских карт*
- *Интернет-мошенничества*
- *Мобильные мошенничества*
- *Финансовые пирамиды*

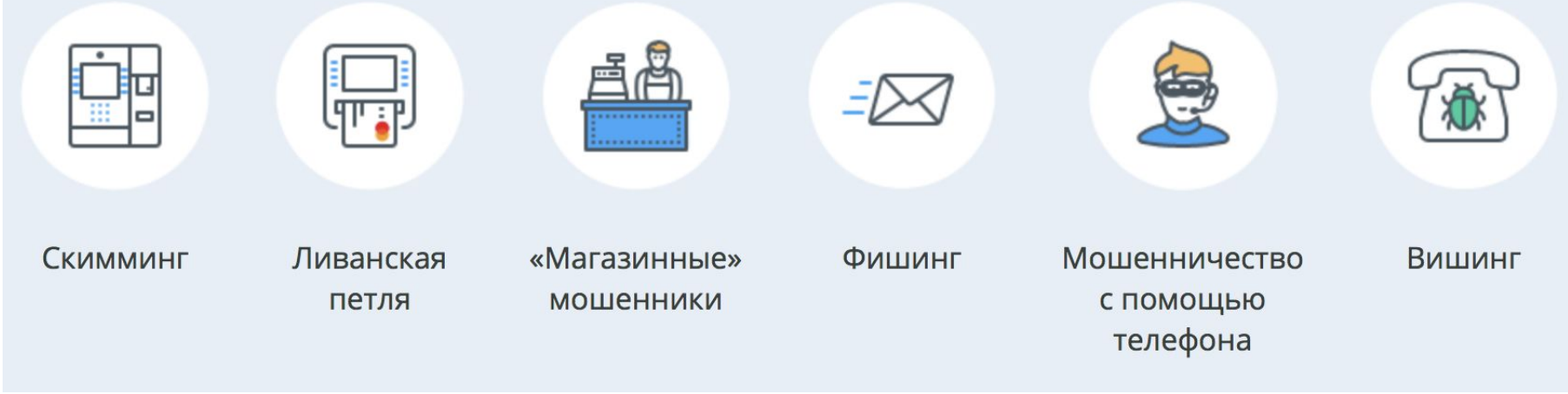
Способы финансового мошенничества с банковскими картами

- Мошенники не знают реквизиты банковской карты: владелец карты сам совершает действия по переводу средств со своей карты на счет мошенников

- Мошенники получают обманным путем реквизиты банковской карты: кража с карты осуществляется с помощью технических средств (скимминг), фишинга, претекстинга (социальной инженерии)

- Мошенники крадут данные / карту без участия владельца: кража данных – с серверов реальных интернет-магазинов, через недобросовестных сотрудников банка, кража пластиковой карты

Схемы мошенничеств с картами



Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение. При этом преступники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать. Именно поэтому важно быть в курсе основных приемов, которые используют злоумышленники, и соблюдать базовые правила безопасности.

Скимминг

- Предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.

Таковыми выступают накладная клавиатура (очень похожая на настоящую) и устройство для считывания данных карты, которое устанавливается на картридер	Вместо клавиатуры может быть установлена миниатюрная камера, которая заснимет процесс ввода ПИН-кода.

При использовании банкомата осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних предметов.

Траппинг (ливанская петля)

- или помощь прохожего. Суть этого вида мошенничества заключается в установке на банкомат устройства, которое **блокирует карту и не выдает ее обратно.**
- Отрезок фотопленки (складывается пополам, края загибаются под углом в 90 градусов) вставляется в банкомат. На нижней стороне фотопленки вырезан небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно.

На помощь человеку приходит «добрый» мошенник, раздавая различные советы. В процессе «помощи» растерянный человек обычно соглашается на введение ПИН-кода, который и запоминает преступник. После чего мошенник «уходит», советуя обратиться в банк. Растерянный человек оставляет карту в банкомате, а мошенник спокойно ее достает и использует по своему усмотрению.

Закрывайте рукой клавиатуру при вводе ПИН-кода

Магазинные мошенничества

- От недобросовестных сотрудников в организациях не застрахован никто. Данные карты могут быть считаны и зафиксированы ручным скиммером, а впоследствии использованы для хищения денег.

  - **Не передавайте карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/ CVC-код) могут быть использованы для чужих покупок**
  - **Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам)**

Фишинг

- Цель фишинга — получить данные о пластиковой карте от самого пользователя. В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.
- При этом мошенники просят доверчивых пользователей возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код. Сделать это предлагается несколькими способами: либо отправив ответное письмо, либо пройдя на сайт банка-эмитента и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.
- **Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте свой ПИН-код.**

Мошенничество с помощью телефона

- Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.
- Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.
- В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя.

Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Вишинг (голосовой фишинг)

- *Новый вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.*
- Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

- Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.
- Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона.
- Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как CVV-код, срок действия карты, дата рождения, номер банковского счета и т. п.

Меры безопасности

- Несмотря на все системы информационной безопасности банка в результате мошеннических операций с картами существует отличная от нуля вероятность хищения средств с вашей карты. Чтобы избежать исчезновения денег, соблюдайте правила, затрудняющие неправомерные операции с вашими финансами:
- Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже -заблокируйте карту
- Сохраняйте все документы до окончания проверки правильности списанных сумм
- Сообщайте банку актуальные контактные данные
- Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки
- Помимо любой личной информации никогда не говорите «да», «нет» или «я». Впоследствии слова могут быть записаны и использованы в незаконных банковских операциях.

Социальная инженерия – как нами манипулируют

- **Приемы социальной инженерии**

1. Предъявляется «приманка», формирующая положительные (выигрыш в лотерею, оплата выставленного вами на продажу товара), или негативные эмоции (претензия по неоплаченному налогу, взыскание по долгу коллекторским агентством, несанкционированное списание средств со счета, блокировка карты).
2. Злоумышленник представляется сотрудником государственных органов, банка, страховой компании, электронного магазина и т.д
3. Создается дефицит времени для принятия решения: «чтобы приз не ушел к другому, перезвонить или сообщить свои данные нужно в ближайшие пять минут», «чтобы избежать повестки суд, необходимо оплатить задолженность в течение 24 часов» и т.д.

- **Результат**
- В условиях необходимости быстрого реагирования наш мозг автоматически переводится в режим стресса. Мы следуем инструкциям мошенников

Социальная инженерия – что делать в ответ

- **Во-первых**, необходимо осознать, что тебя ставят в условия немедленного принятия решения, и зажечь «красную лампочку». Покупки-продажи финансовых продуктов и услуг не должны совершаться в течение ближайших 5 минут.
- **Во-вторых**, необходимо любыми способами убрать влияние дефицита времени, взять паузу. Если собеседник говорит вам «Сейчас или никогда!», смотри пункт первый.
- **В-третьих**, успокоиться и трезво оценить ситуацию:
- • медленно подышать – это один из способов снизить частоту пульса и перевести свой организм и мозг из режима быстрого реагирования в спокойный режим;
- • проверить информацию, которую вы успели получить от звонившего (посмотреть в сети Интернет информацию об аналогичных ситуациях или позвонить по официальному номеру в компанию от имени которой вас ожидают призы или угрозы;
- • позвонить родным, другу, кому-то, кто мог бы посмотреть на ситуацию взглядом, не замутненным эмоциями, и указать вам на риск мошенничества.

Другие виды мошенничества

- Интернет мошенничество
- Мобильное мошенничество

«Вы выиграли приз...»

«Мама, я попал в аварию...»

«Ваша банковская карта заблокирована...»

Вирус

Способы защиты

- Не отвечайте на СМС от неизвестных абонентов, в том числе поздравительные сообщения и открытки. С вашего счета могут списать деньги.

- При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию. Банк никогда не сообщает подобным образом информацию.

- Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения. Это можно сделать на сайте своего оператора мобильной связи.

Как не стать жертвой финансовой Пирамиды

- Если говорить о деньгах, то нами движут два основных чувства: страх потерять заработанное и желание максимально преумножить то, что уже есть. К сожалению, часто именно второе чувство притупляет осторожность и приводит к плачевным финансовым результатам.
- Финансовая пирамида – схема инвестиционного мошенничества, в которой доход по привлеченным денежным средствам образуется не за счет вложения их в прибыльные активы, а за счет поступления денежных средств от привлечения новых инвесторов.

Признаки пирамиды

- Не поддавайтесь на агрессивную рекламу «лёгких и быстрых денег». Прежде чем принять решение о вложении денег, проверьте поступившее вам предложение на признаки финансовой пирамиды:

- Призыв не раздумывать и вкладывать быстро
- Обещание сверхвысокой доходности больше 20% годовых
- Объяснение такой доходности непрозрачными сверхприбыльными проектами
- Обещание вознаграждения за приведенных клиентов
- Анонимность организаторов и отсутствие защиты прав вкладчика в договоре
- Отсутствие информации о возможны рисках
- Требование , например, оплатить «вступительный взнос», «обучение», «участие в семинаре»
- Отсутствие лицензии/ указание номера чужой лицензии, или собственной, но не позволяющей работать с денежными средствами

СПАСИБО ЗА ВНИМАНИЕ!