КОНКУРС ПРОЕКТОВ ОБУЧАЮЩИХ МАТЕРИАЛОВ «ТВОЯ ФИНАНСОВАЯ БЕЗОПАСНОСТЬ»

студентка 2 курса Частного образовательного
учреждения профессионального образования
Брянский техникум управления и бизнеса
Рябых Злата Павловна
(номер телефона 8-900-363-73-36)

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

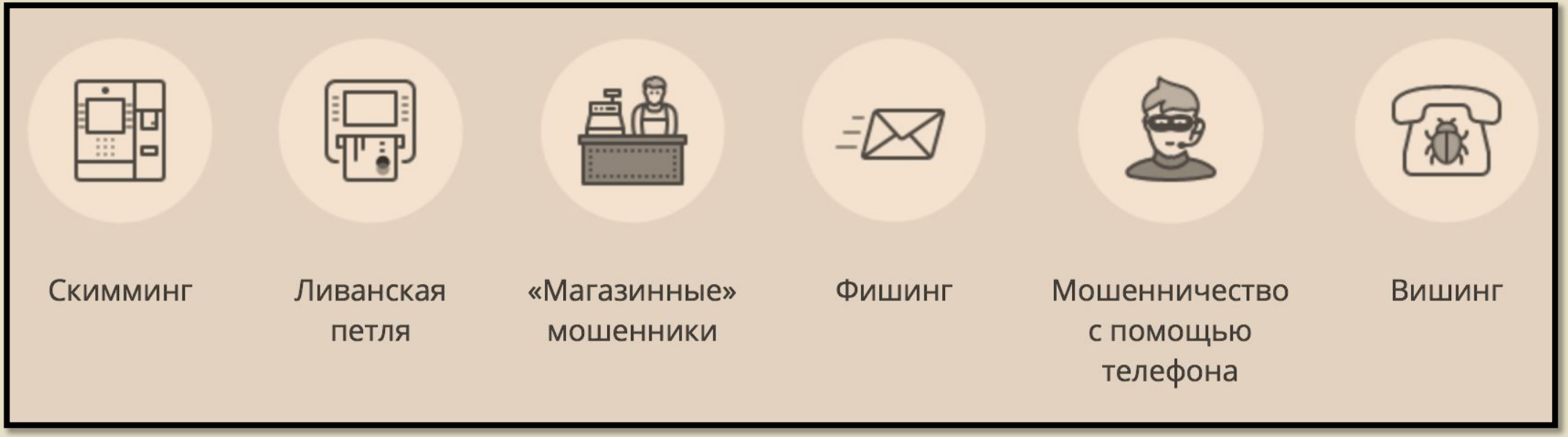
Мошенничества с использованиям банковских карт

Банковская карта – удобный инструмент повседневных расчетов.

- Дебетовые - инструмент управления банковским счетом, на котором размещены собственные средства держателя карты.

- Кредитные - это банковская пластиковая карта, позволяющая на основании заключенного с банком договора брать в долг у банка определенные суммы денег

СХЕМЫ МОШЕННИЧЕСТВА С КАРТАМИ



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

- 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

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,

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

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

ПРИ РАСЧЕТЕ КАРТАМИ

- **Не превышайте лимит кредитования – это может приводить к блокированию карты, штрафам и комиссиям**
- **Своевременно оплачивайте кредит – это обеспечит отличную кредитную историю и убережет от штрафов**
- **Не допускайте потери карты, поломки, блокировки - перевыпуск карты может стоить дополнительных средств**
- **Не снимайте с карты деньги полностью – оставьте сумму для оплаты комиссий или автоматических платежей. В случае отсутствия суммы и если карта предусматривает овердрафт, банк совершит данный платеж за счет заемных средств.**
- **Если сменили место работы уточните**

РЕКОМЕНДАЦИИ

- Проявляйте бдительность и внимательность к своим ежедневным финансовым операциям.
- Никогда никому не сообщайте ваши пароли, ПИН-код, CVV.
- Используйте антивирусное программное обеспечение.
- При совершении платежей в интернете обязательно проверяйте, какой URL стоит в адресной строке
- Не передавайте банковскую карту третьим лицам.
- Обязательно установите пароль для разблокировки телефона, особенно если на нем установлено банковское мобильное приложение.
- Гарантирование доходности по инвестициям, в несколько раз превышающей

ТЕСТ

1) Как можно сделать использование банковской карты максимально безопасным:

1. Никогда не сообщать третьим лицам PIN/CVV/CVC-2 код, в том числе и сотрудникам банка
2. Отправлять фотографию карты с двух сторон тем, кто хочет перевести мне деньги
3. Подключить СМС-информирование, чтобы точно знать, когда происходит операция по карте
4. Сообщать посторонним лицам одноразовый пароль, который приходит по СМС
5. Заблокировать карту при обнаружении ее пропажи
6. Написать ПИН-код непосредственно на карте, чтобы не забыть его и случайно не заблокировать карту

2) Как безопасней оплачивать товары и услуги через сеть:

1. С помощью своей зарплатной карты, чтобы заработать дополнительные бонусы
2. С помощью кредитной карты
3. С помощью специальной карты для покупок в Интернете

3. Что не является финансовым мошенничеством?

1. Вам сообщают, что вы выиграли приз и просят вас внести регистрационный взнос за выигрыш
2. Центральный банк РФ сообщает вам, что ваша банковская карта заблокирована
3. Сотрудник банка просит вас назвать PIN-код вашей банковской карты
4. При обращении вами в колл-центр банка, вас просят назвать кодовое слово или паспортные данные
5. Все описанные ситуации являются мошенничеством

4. Перечислите способы защиты от интернет-мошенников:

2. Никогда и никому не сообщать пароли
3. Сообщать пароли только сотрудникам банка
4. Никогда не делать копий файлов с секретной информацией
5. Не открывать сайты платежных систем по ссылке (например, в письмах)
6. При поиске удаленной работы не реагировать на просьбы оплаты каких-либо регистрационных взносов


Спасибо за внимание