



ОСТОРОЖНО:

МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ЦЕЛЬ

- выработка личной стратегии грамотного поведения в ситуации мошеннических действий.

ЗАДАЧИ

- 1. Дать определение понятию «мошенничество»
- 2. Рассмотреть основные виды мошенничества и методы финансовых мошенников
- 3. Выявить «зоны риска» встречи с финансовыми мошенниками
- 4. Выстроить собственную линию поведения, чтобы не стать жертвой мошенников.

ПРЕДМЕТНЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

- Дать определение финансового мошенничества.
- Изучить наиболее распространенные виды финансовых мошенничеств.
- Выработать способы защиты от мошенничества.

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

- Совершение противоправных действий в сфере денежного обращения путём обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.
- Существует много видов мошенничества. На сегодняшний день наиболее распространены мошеннические действия в киберпространстве. Кто скажет, что такое киберпространство?

ВИДЫ МОШЕННИЧЕСТВА

Как_защититься_от_кибермошенничества_Презентация_Весна_2022.pdf - Adobe Acrobat Reader DC (32-bit)

Файл Редактирование Просмотр Подпись Окно Справка

Главная Инструменты Как_защититься_о... x Войти

 Банк России

КИБЕРПРОСТРАНСТВО-ЭТО...

Среда информационного взаимодействия и обмена данными в компьютерных сетях и сетях связи.

Элементы киберпространства:

серверы, компьютеры, мобильные гаджеты, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети.



Классный час РЕ... X P W Классный час M... Как_защититься_... RU 22:57 31.03.2022

ФИШИНГ

- Получение персональных данных любым доступным способом. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих. Вам могут прислать письмо якобы от вашего банка или почтового сервера, которым вы пользуетесь, и сообщить, что произошли какие-то изменения (вас добавили в черный ящик, заблокировали карту, кто-то завладел вашим паролем и т.п.). При клике на ссылку вы переходите на сайт, который внешне почти ничем не отличается от сайта реальной компании, но если присмотреться, то можно заметить отличия.

СМИШИНГ

Выманивание данных карты мошенниками при обращении в социальных сетях. К вам обращаются от лица вашего друга или родственника, взломав его страницу, и просят одолжить деньги или сказать код-пароль, который пришел в sms на ваш телефон.

Также есть такие мошенники, которые звонят пожилым людям и разыгрывают спектакль, что якобы их дети или внуки попали в аварию и просят передать через 3-е лицо крупную сумму денег, иначе им не сделают вовремя медицинскую операцию или посадят в тюрьму.

ТЕЛЕФОННЫЕ МОШЕННИКИ

Как защититься от кибермошенничества Презентация Весна_2022.pdf - Adobe Acrobat Reader DC (32-bit)

Файл Редактирование Просмотр Подпись Окно Справка

Главная Инструменты Как_защититься_о... x Войти

 Банк России

ТЕЛЕФОННЫЕ МОШЕННИКИ

- Звонок якобы от имени банка или правоохранительных органов: вас просят сообщить личные данные.
- СМС или письмо якобы от банка с просьбой перезвонить.
- СМС об ошибочном зачислении средств или с просьбой подтвердить покупку.
- СМС от имени родственников, которые просят перевести деньги на неизвестный счет.



Переведи мне деньги

RU 23:26 31.03.2022

Классный час РЕ... X P W Классный час М... Как защититься...

ВИДЫ ТЕЛЕФОННЫХ МОШЕННИКОВ

Ненадежные интернет-магазины. Мошенники могут создать сайт несуществующего интернет-магазина (или скопировать реальный сайт). Вы оплачиваете свои покупки, а товар не получаете.

Мошенничества на сайтах объявлений продажи товаров (типа «Авито»). Выставляете на сайте объявление о продаже товара. С вами связывается «Покупатель» и просит сообщить ему данные карты, чтобы зачислить на нее деньги.

БЕЗОПАСНОСТЬ СРЕДСТВ

- Безопасность средств на своей банковской карте, в первую очередь, это твоя зона ответственности . Если по неосторожности разгласить важную информацию о своей карте, то банк, скорее всего, не будет возмещать средства, поэтому нужно быть бдительным и помнить о правилах безопасности.

ПРАВИЛА БЕЗОПАСНОСТИ



Электронные платежи

Основные правила безопасности

- Никому не сообщайте ваш пароль. Не храните его на компьютере
- Проверяйте, что соединение происходит на защищенном сайте («https://»)
- Убедитесь, что компьютер не заражен вирусами



Основное правило – пользуйтесь проверенными (знакомыми) сервисами и сайтами

СКИММИНГ

- Вид мошенничества, при котором третьи лица заведывают электронными данными карты и пин-кодом с помощью технических приборов, расположенных на банкомате (накладная клавиатура, накладка на картоприемник и прочее).

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

- 1. Никогда никому не сообщать свой пароль, включая сотрудников платежных систем. Никогда не сохранять информацию о своем пароле на любых носителях, в том числе и на компьютере. Если есть подозрения, что кто-либо получил доступ к личному кабинету, сменить пароль или заблокировать свой счет/аккаунт.
- 2. Нельзя вводить данные карты на сомнительных сайтах
- 3. Убедиться, что компьютер не поражен какими-либо вирусами. Установить и активизировать антивирусные программы. Стараться их постоянно обновлять, так как действие вирусов может быть направлено на передачу третьим лицам информации о вашем пароле.

СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ



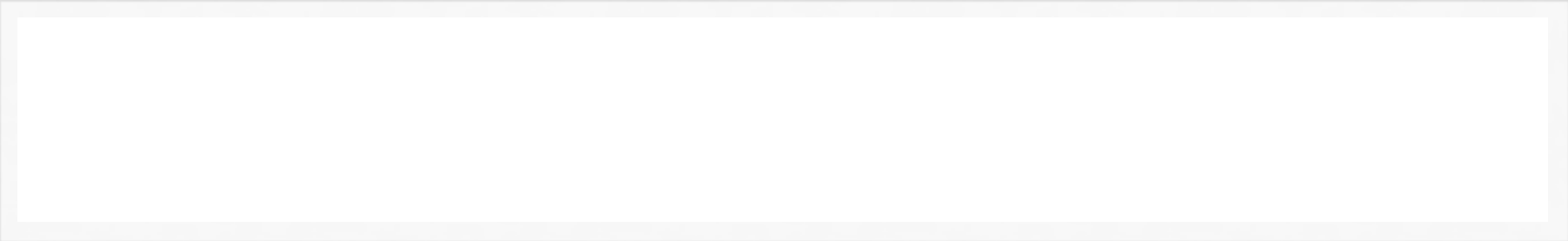
Банк России

- Всегда проверяйте информацию.
- Не переходите по неизвестным ссылкам.
- Если вам сообщают, будто что-то случилось с родственниками, срочно свяжитесь с ними напрямую.
- Не перезванивайте по сомнительным номерам.
- Не храните данные карт на компьютере или в смартфоне.
- Не сообщайте никому личные данные, пароли и коды.
- Установите антивирус на компьютер себе и родственникам

Объясните пожилым родственникам эти простые правила и будьте бдительны!!!

ПОДВЕДЕНИЕ ИТОГОВ

- **Если вдруг случилась беда, куда обращаться за помощью?**
- Нужно идти в отделение полиции с паспортом, сообщить дежурному о факте мошенничества и написать заявление.
- **Будьте внимательны, мошенники с каждым годом становятся все изощреннее в своих способах отъема денег. Наивно полагать, что они способны обхитрить только пожилых людей или несовершеннолетних детей. В их арсенале полно уловок! Главное, не поддаваться первому порыву, все обдумать или лучше всего все рассказать и посоветоваться со взрослыми.**



- **Спасибо!**