Банк России

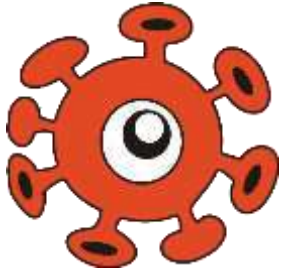
КИБЕРБЕЗОПАСНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

СЕГОДНЯ ВЫ УЗНАЕТЕ:

Какие виды мошенничества существуют в сети Интернет.

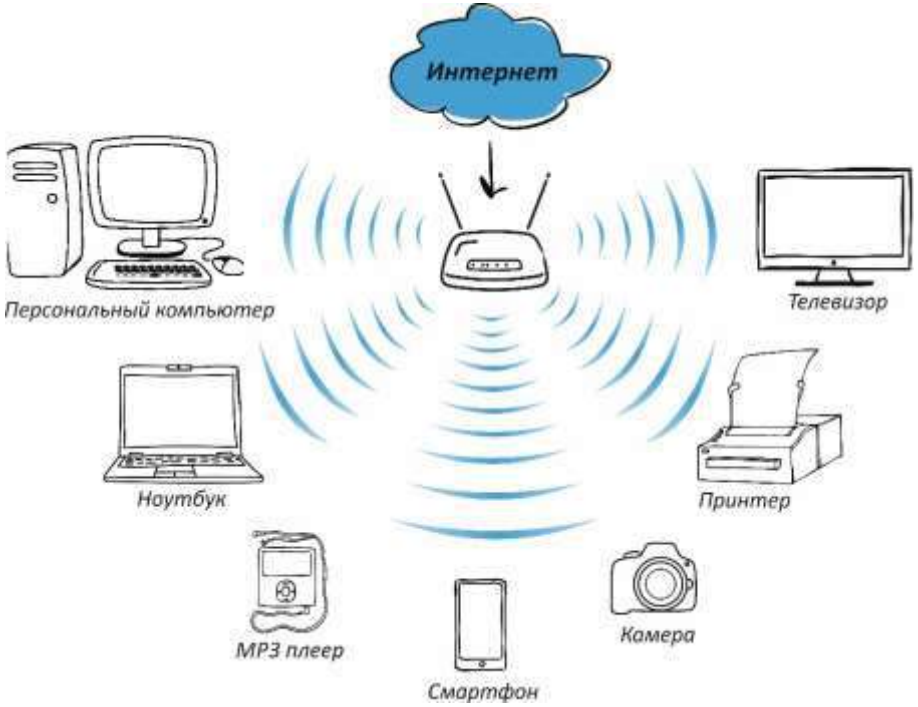
Способы похищения злоумышленниками конфиденциальной информации о вас и ваших электронных средствах платежа.

Какие приемы социальной инженерии используют мошенники, чтобы завладеть вашими денежными средствами.



ЧТО ТАКОЕ КИБЕРПРОСТРАНСТВО?

КИБЕРПРОСТРАНСТВО –



это среда информационного взаимодействия и обмена данными в компьютерных сетях и сетях связи.

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

ЭЛЕКТРОННЫЙ БАНКИНГ (E-BANKING) –

это оказание банковских услуг с использованием возможностей глобальной сети Интернет и мобильной связи.

- **PC-банкинг** – удаленное управление своим банковским счетом с помощью компьютера.

- **Мобильный банкинг** – удаленное управление своим банковским счетом с помощью мобильного телефона или смартфона.

- **POS-терминалы** и **банкоматы** – с их помощью мы оплачиваем покупки в магазинах.

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (ВПО)

Вирусы

Трояны

Черви

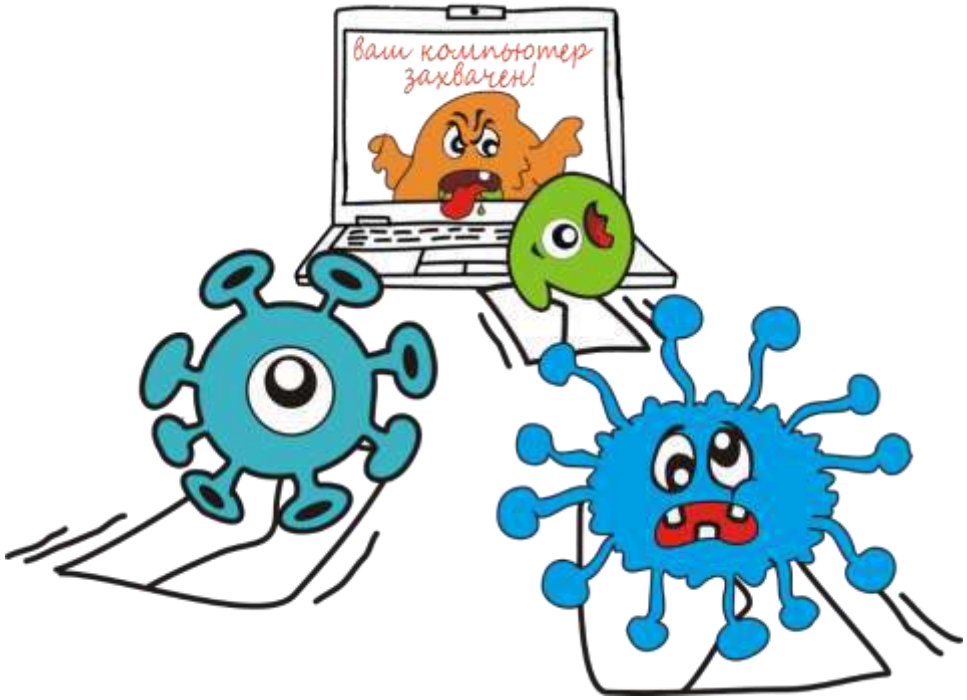
Руткиты

ЧТО НЕЛЬЗЯ ДЕЛАТЬ ПОЛЬЗОВАТЕЛЮ

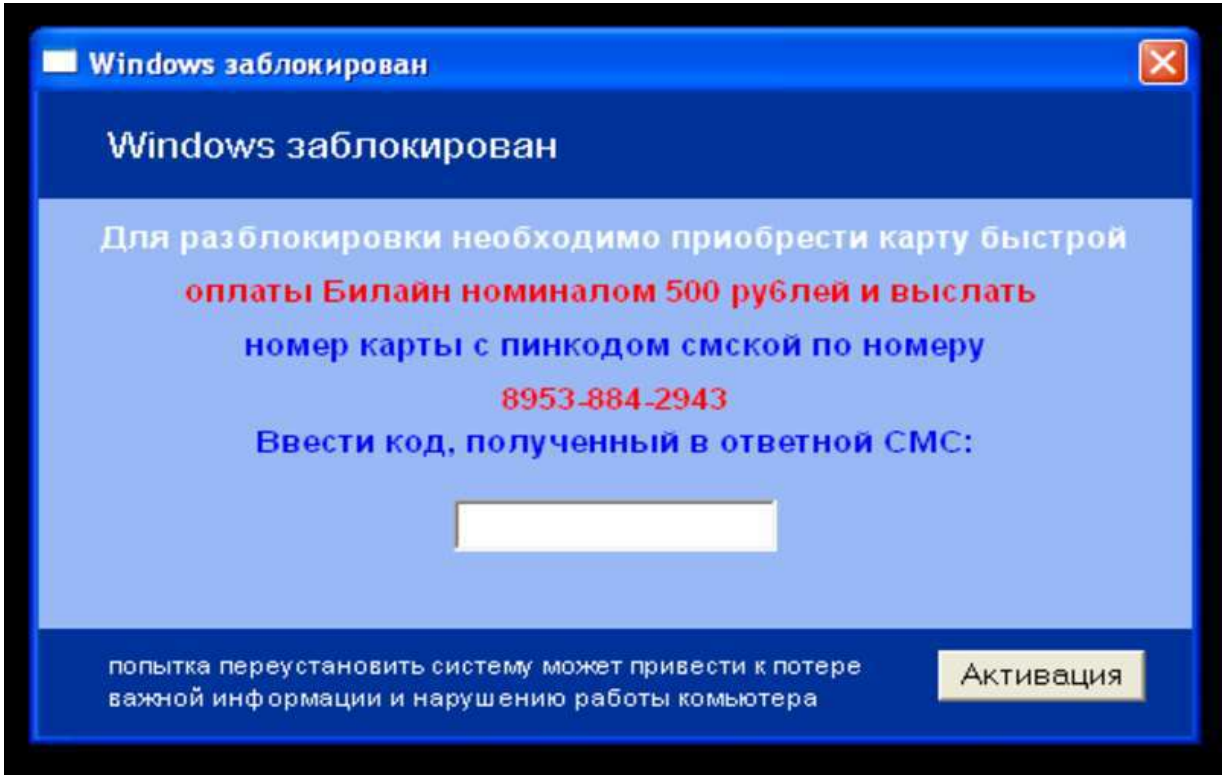
- **Переходить** по подозрительным ссылкам в электронной почте или в браузере.
- **Открывать** подозрительные вложения.
- **Скачивать** и **устанавливат**ь «пиратское» ПО.
- **Использовать** непроверенные флешки, смартфоны и др.

ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР

- **Похищает** информацию.
- **Участвует** в атаках.
- **Блокирует** работу



ПРИМЕР БЛОКИРОВКИ КОМПЬЮТЕРА



КАКИЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРОВ И СМАРТФОНОВ НАРУШАЮТ ПРАВИЛА БЕЗОПАСНОСТИ?

1. Использование чужих устройств для входа в мобильный банк, Интернет-банк, покупок в Интернете и сохранение на них личных данных.
2. Проверка флэшек на наличие опасных программ.
3. Переход по подозрительным ссылкам.
4. Немедленное отключение всех услуг при утрате телефона или планшета, к которым подключено смс-информирование или мобильный банк.

A. 1, 4

B. 1, 3

C. 2, 3

ФИШИНГ

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей и их деньгам

РЕКЛАМА МОШЕННИЧЕСКОГО СЕРВИСА

Истории успеха, рассказанные на Youtube

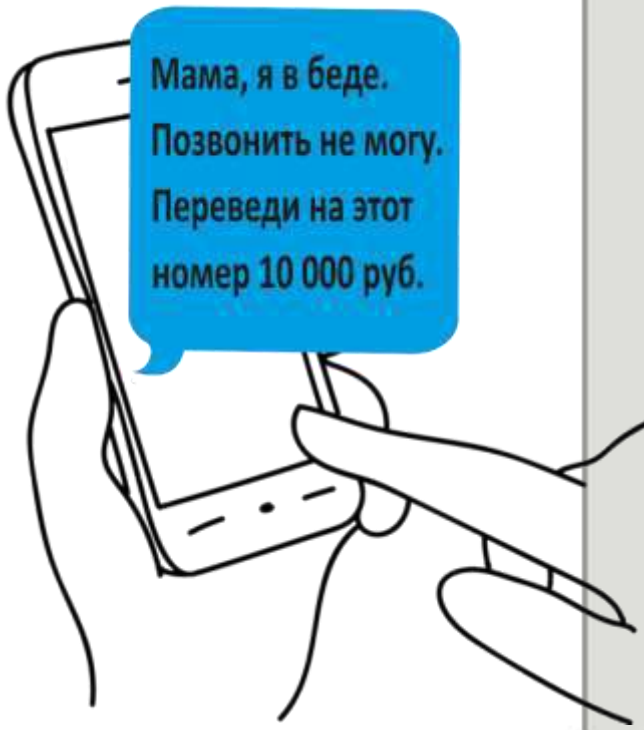
- Посмотрите дату регистрации, как правило, канал будет относительно молодой.
- Размещено небольшое количество роликов, причем самые первые из них будут на совершенно другую тематику.
- Последний ролик с рекламой мошеннического сервиса будет опубликован совсем недавно.

ПРИЗНАКИ ФИШИНГОВОГО САЙТА

- Доменное имя похоже на название известного интернет-магазина, банка, социальной сети, бренда, но отличается на несколько символов.
- Нет префикса **https**: **s** - secure - безопасное соединение.
- Опечатки, несоответствия, небрежности и ошибки, очень низкие цены.
- На странице оплаты отсутствуют логотипы программ MasterCard SecureCode и Verified by Visa, использующих технологию 3D-Secure.
- Ссылка пришла из неизвестного источника - СМС или социальные сети.
- Вы попали на сайт при использовании открытой сети Wi-Fi без пароля.

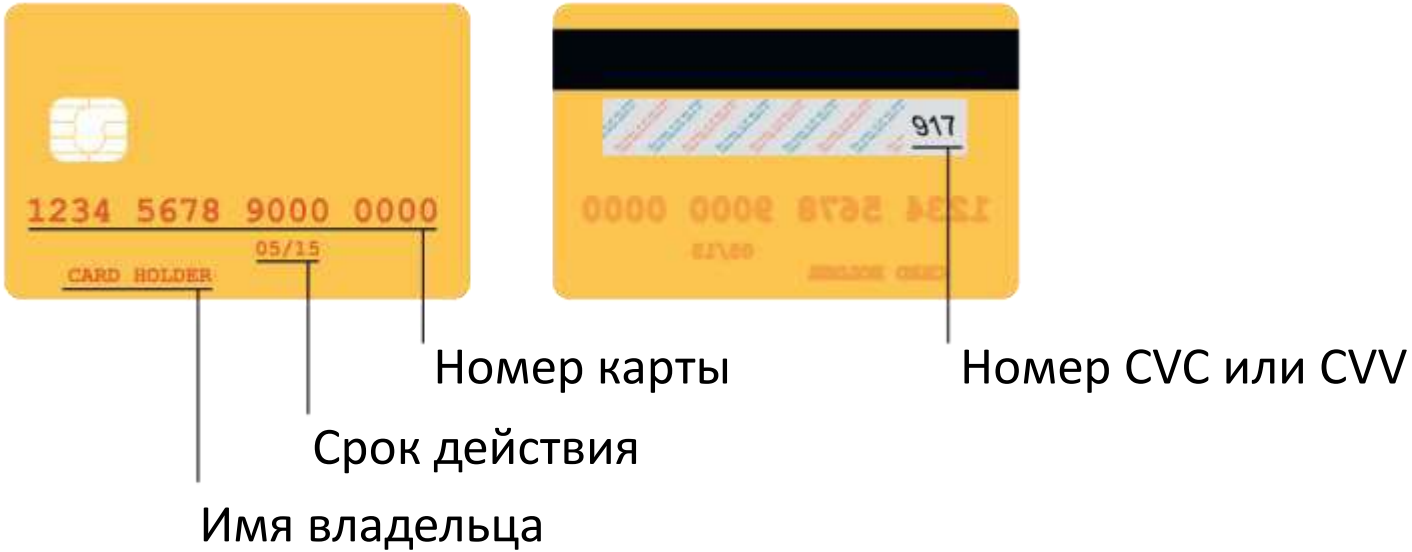
ТЕЛЕФОННЫЕ МОШЕННИКИ

- Звонок якобы от имени банка: 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.



МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам **нужны:**



БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ

ЗА

- высокая скорость выполнения платежной операции
- удобство для операций **до 1000** рублей (как правило) – можно не вводить ПИН-код

ПРОТИВ

- карту могут украсть и оплачивать недорогие покупки/услуги без ПИН-кода
- возможны мошенничества с платежными терминалами *(считывающие устройства на расстоянии)*

РЕКОМЕНДАЦИИ: установить суточный лимит и смс-уведомления

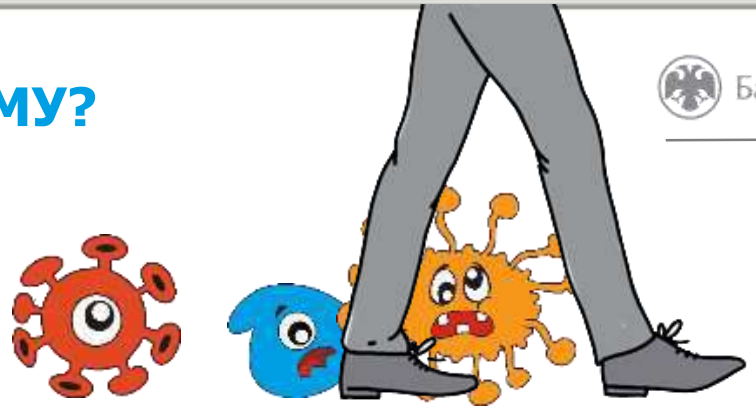
КАК И ГДЕ МОГУТ УКРАСТЬ ВАШИ ДАННЫЕ?

В кафе или магазине — сотрудник-злоумышленник может сфотографировать вашу карту.

В банкомате — на нем мошенники могут установить скиммер и видеокамеру.

ТАК МОЖЕТ ВЫГЛЯДЕТЬ БАНКОМАТ СО СКИММЕРОМ

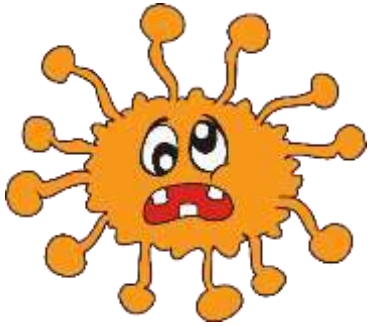
КАК ОБОЙТИ ПРОБЛЕМУ?



- Используйте банковскую карту только в тех местах, которые заслуживают доверия
- Осмотрите банкомат. На нем не должно быть посторонних предметов
- Набирая ПИН-код, прикрывайте клавиатуру рукой
- При наборе ПИН-кода вводимые цифры не должны отображаться (****)
- Подключите мобильный банк и СМС-уведомления
- Никому не сообщайте секретный код из СМС
- Не теряйте карту из виду (в магазине, кафе)

С МОЕЙ КАРТЫ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

- Позвоните в банк и **заблокируйте карту**
- Запросите выписку по счету и **напишите заявление о несогласии с операцией**
- Обратитесь в полицию



Как не стать жертвой киберпреступников?

СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

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

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