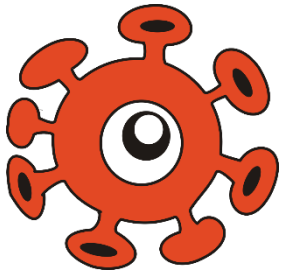
Банк России

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИЧЕСТВА:

СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОЙ СРЕДЕ.

СЕГОДНЯ НА УРОКЕ ВЫ УЗНАЕТЕ:

- Что такое киберпреступность и как она появилась;
- Какие виды мошенничества существует в сети;
- Какие приемы социальной инженерии используют мошенники;
- Как защититься от фишинга и других видов кибермошенничества.



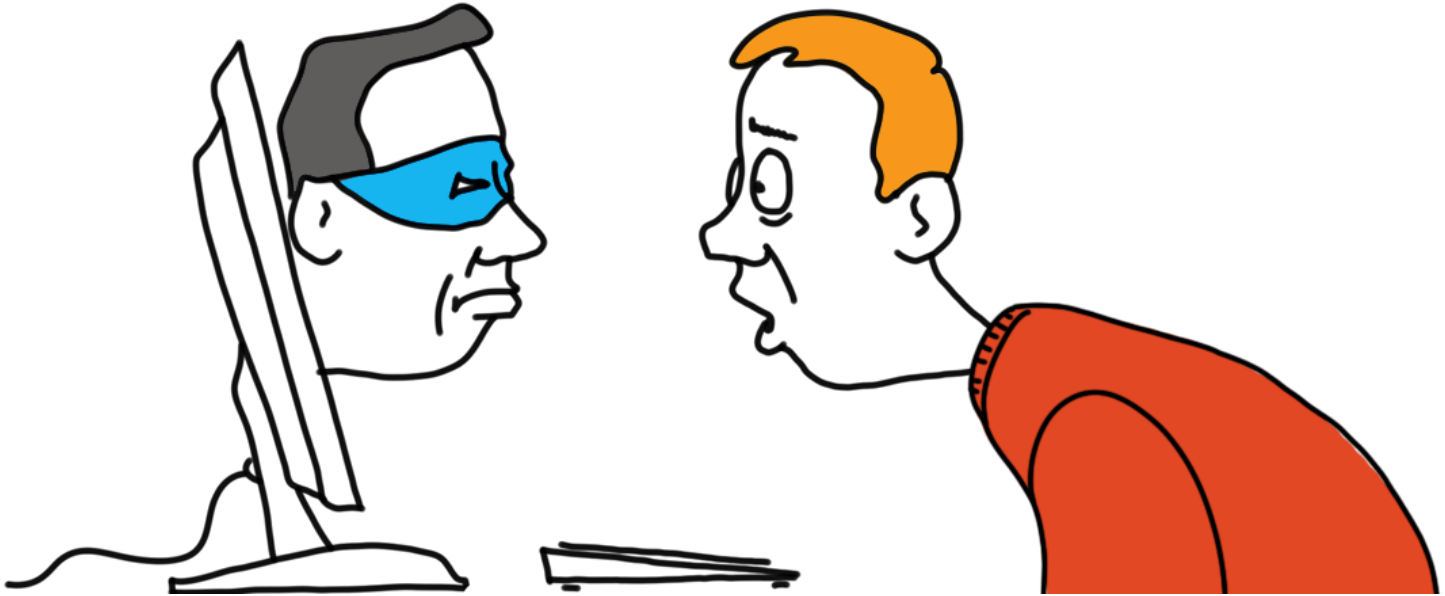
Интерактив

ЧТО ТАКОЕ КИБЕРПРЕСТУПНОСТЬ?

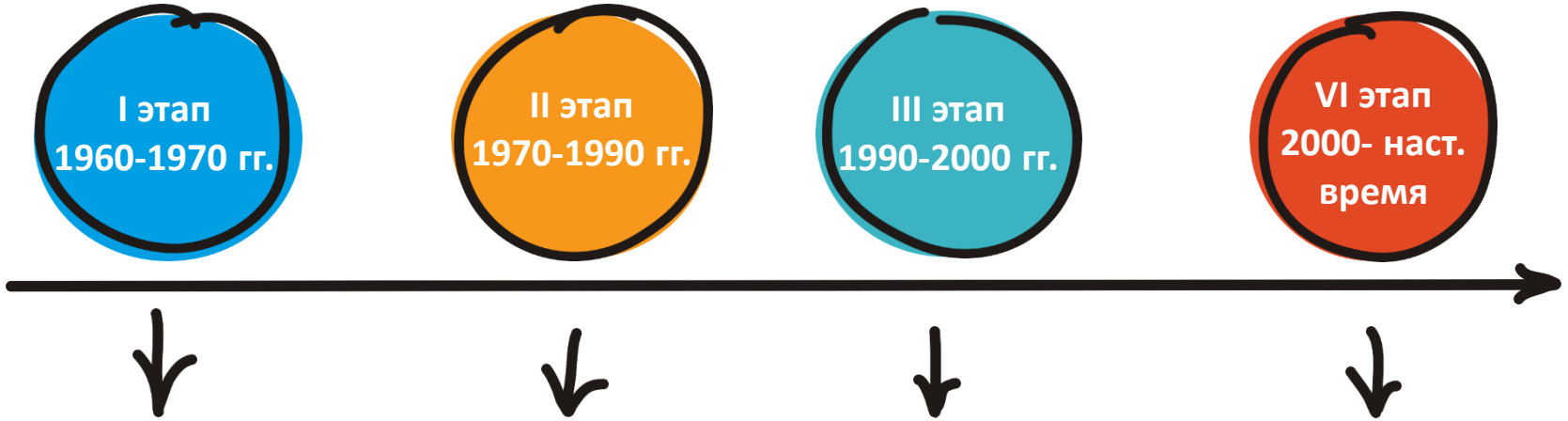
Напишите ответ в чат

КИБЕРПРЕСТУПНОСТЬ – ЭТО…

незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей.



ИСТОРИЯ ВОЗНИКНОВЕНИЯ КИБЕРПРЕСТУПНОСТИ



Разработка и распространение сети Интернет. Компьютерная преступность не развита.

Становление компьютерных преступлений, появление субкультуры хакеров.

Использование преступниками IT технологий для совершения преступлений.

Возникновение кибертерроризма и международных хакерских группировок. Киберпреступность приобретает транснациональный характер.

ЭЛЕКТРОННЫЙ БАНКИНГ (E-BANKING)…

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

PC – банкинг, удаленное управление своим банковским счетом с помощью компьютера

мобильный банкинг, с помощью мобильного телефона или смартфона.

POS-терминалы и **банкоматы**, с помощью которых мы оплачиваем покупки в магазинах.

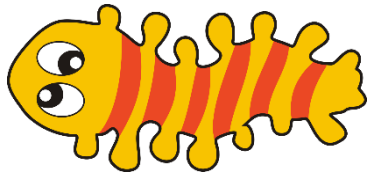
Билл Гейтс, один из создателей и бывший крупнейший акционер компании Microsoft

«Нам нужен банкинг, но не банки»

КАК ВЫ СЧИТАЕТЕ, КАКОЙ ИЗ ВИДОВ ЭЛЕКТРОННОГО БАНКИНГА БУДЕТ НАИБОЛЕЕ ВОСТРЕБОВАН И РАЗВИТ В БЛИЖАЙШЕМ БУДУЩЕМ?

Интерактив

1. Банкинг с использованием персонального компьютера, PC – банкинг
2. Применение банкоматов и различных POS-терминалов.
3. Мобильный банкинг

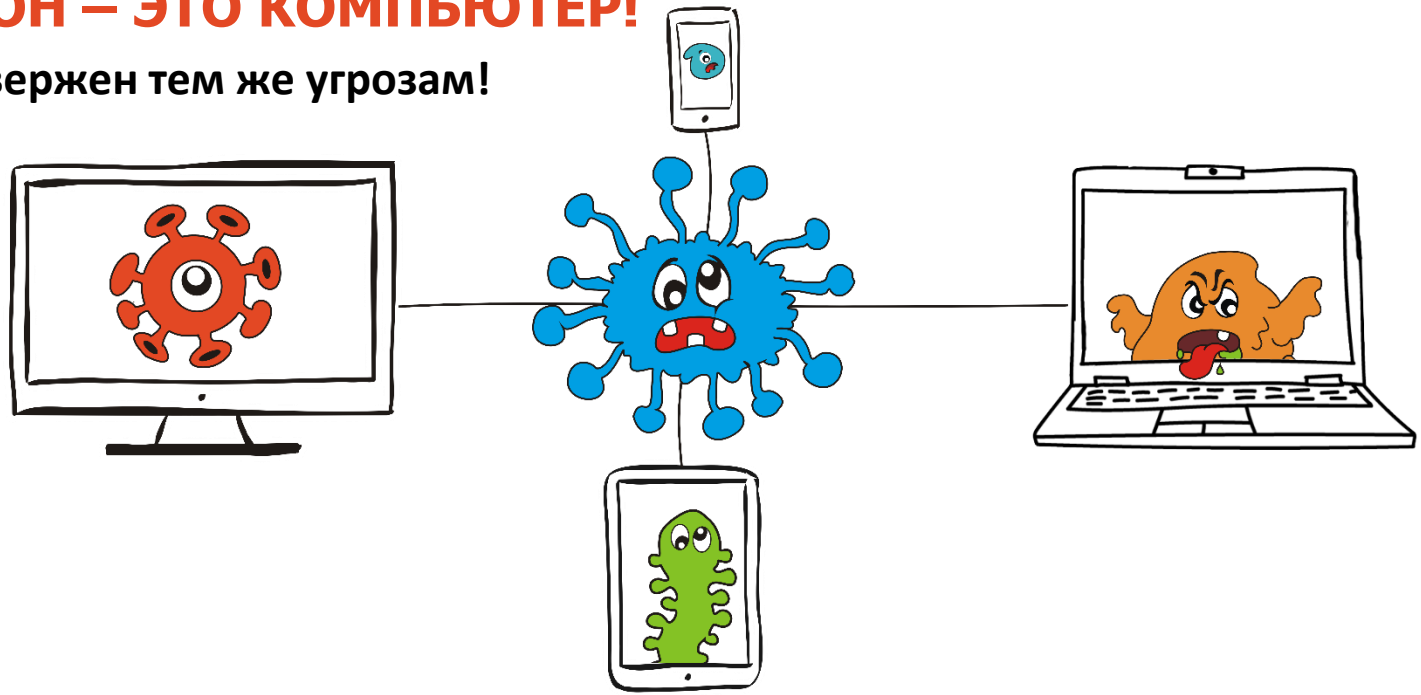


Напишите ответ в чат

ПОЧЕМУ БУДУЩЕЕ ЗА МОБИЛЬНЫМ БАНКОМ

СМАРТФОН – ЭТО КОМПЬЮТЕР!

Подвержен тем же угрозам!

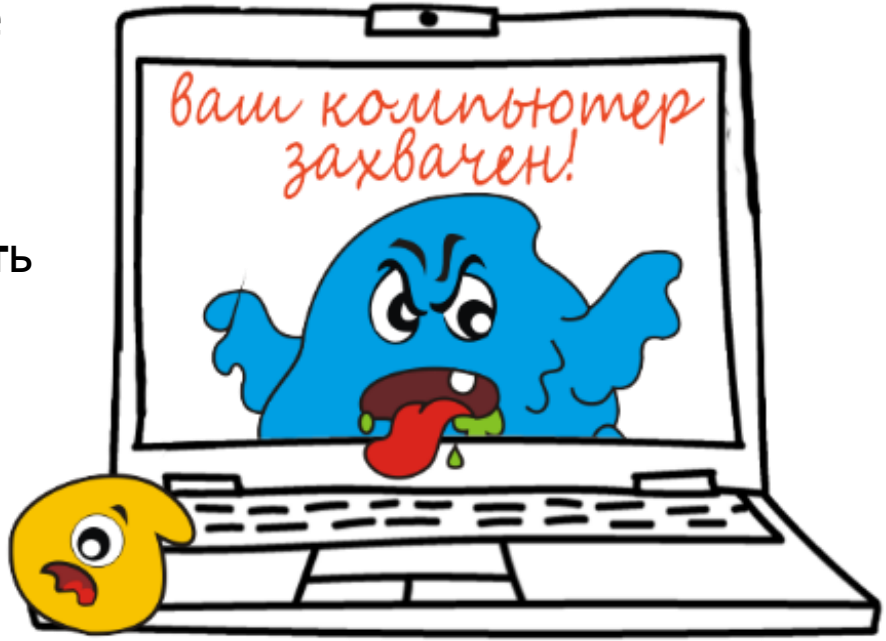


ЧТО НЕЛЬЗЯ ДЕЛАТЬ ПОЛЬЗОВАТЕЛЮ …

Открывать подозрительные вложения.

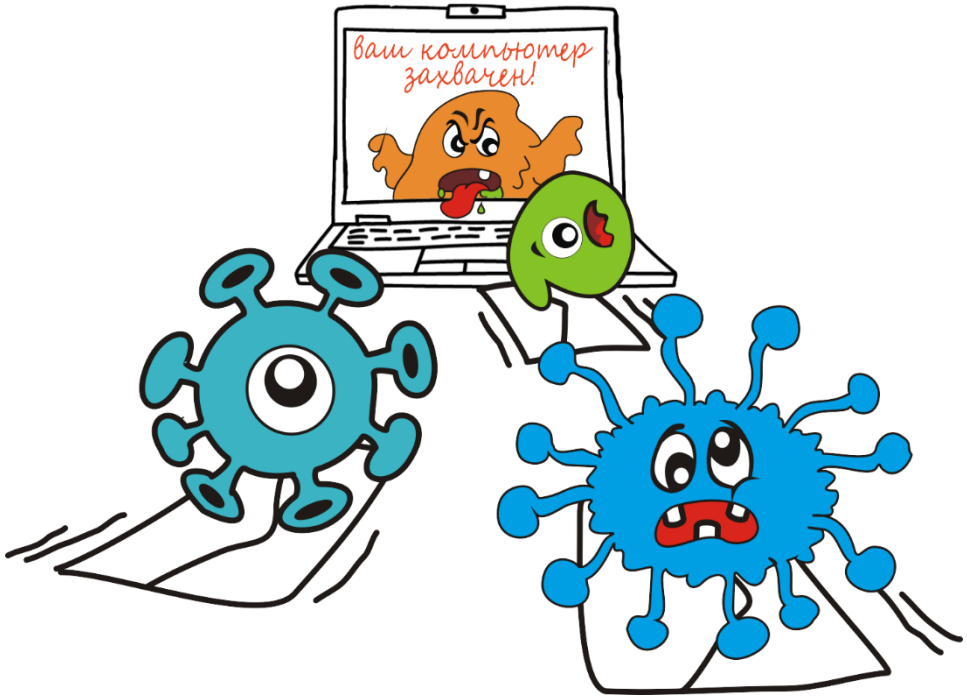
Скачивать и **устанавливать** «пиратское» ПО.

Вставлять непроверенные флешки, смартфоны и др.



ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР

- **Похищает** информацию.
- **Участвует** в атаках.
- **Нарушает** свойства информации.



ВИРУСЫ, РАБОТАЮЩИЕ С СИСТЕМАМИ ОНЛАЙН-БАНКИНГА

На компьютер попадает вредоносное программное обеспечение и начинает выполнять операции в интересах злоумышленника.

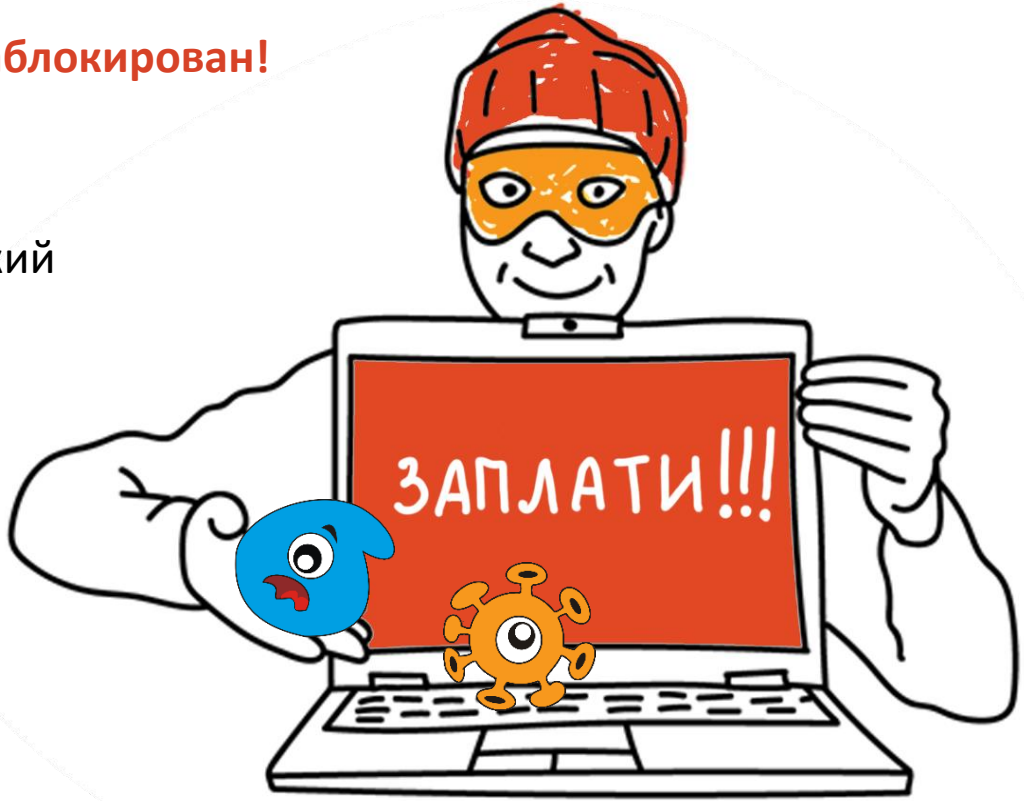
Входит в ваш банковский профиль, используя ваши пароли и получает полный доступ к вашим деньгам.

ПРОГРАММА-ВЫМОГАТЕЛЬ

Файлы зашифрованы! Доступ заблокирован!

НА ЭКРАНЕ ТРЕБОВАНИЕ:

- «Отправьте СМС на короткий номер»
- «Переведите деньги на мобильный счет»
- «Расплатись биткоинами» (электронными деньгами)



Вы купили компьютер с рук. Необходимое программное обеспечение было установлено, вы решили ничего не менять.

Интерактив

КАКИЕ ПРАВИЛА БЕЗОПАСНОСТИ ВЫ НАРУШИЛИ, И К КАКИМ ПОСЛЕДСТВИЯМ ЭТО МОЖЕТ ПРИВЕСТИ?

1. Ничего не случится, я купил компьютер у знакомого, видел его три раза.

2. Обязательное обновление антивируса, ведь вирус может заблокировать онлайн-банкинг или иную систему, в которой вы зарегистрированы.

3. Ничего не произойдёт, при оплате покупок в Интернете я использую отдельную карту.

Напишите ответ в чат

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Мошенникам **нужны:**

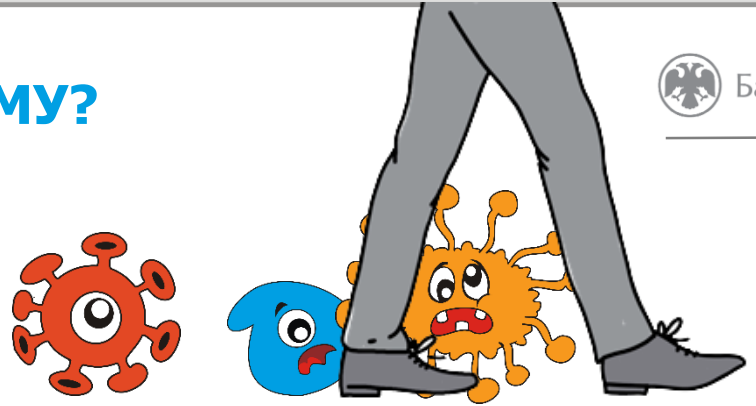
КАК И ГДЕ МОГУТ УКРАСТЬ ВАШИ ДАННЫЕ?

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

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

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).

БЕСКОНТАКТНЫЕ БАНКОВСКИЕ КАРТЫ

ЗА

- высокая скорость выполнения платежной операции
- удобство для операций **до 1000** рублей - можно не вводить пинкод

ПРОТИВ

- карту украли, пользуются ею в магазинах **до 1000** руб. без ПИН-кода
- возможны мошенничества с платежными терминалами *(считывающие устройства на расстоянии)*

РЕКОМЕНДАЦИИ: установить суточный лимит и смс уведомления

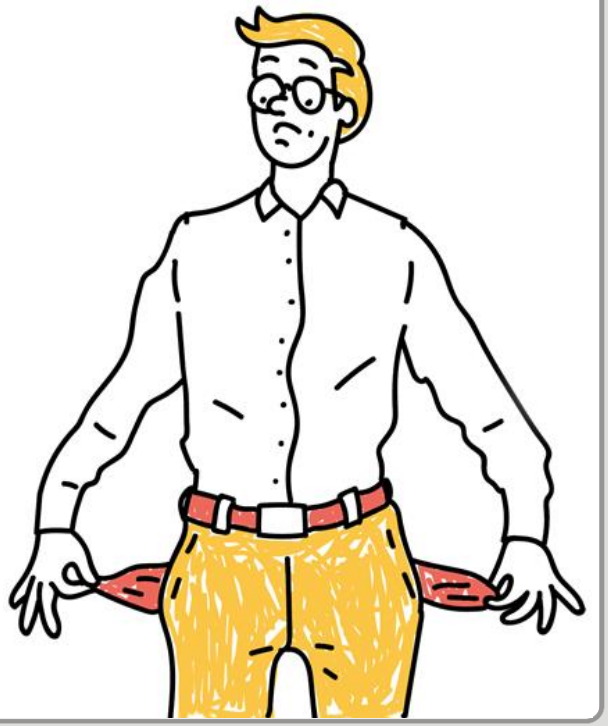
*Петр в кафе расплатился **бесконтактной картой**, доверив ее официанту. На следующий день Петр обнаружил, что **денег на счете нет**.*

Интерактив

КАК ЭТО МОЖНО БЫЛО ИЗБЕЖАТЬ?

Вариантов ответа может быть несколько.

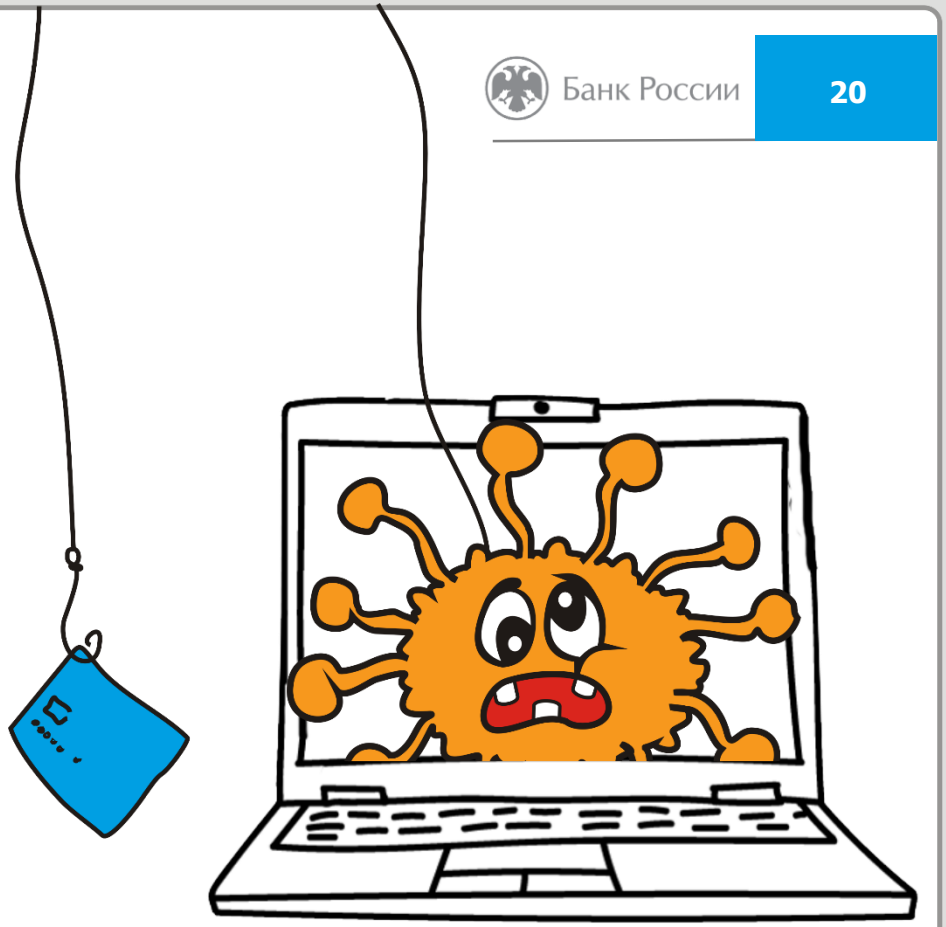
1. Установить смс-оповещение.
2. Попросить девушку расплатиться.
3. Установить лимит суммы, который можно снять без использования пин-кода.
4. Не давать карту в руки официанту.



Напишите ответ в чат

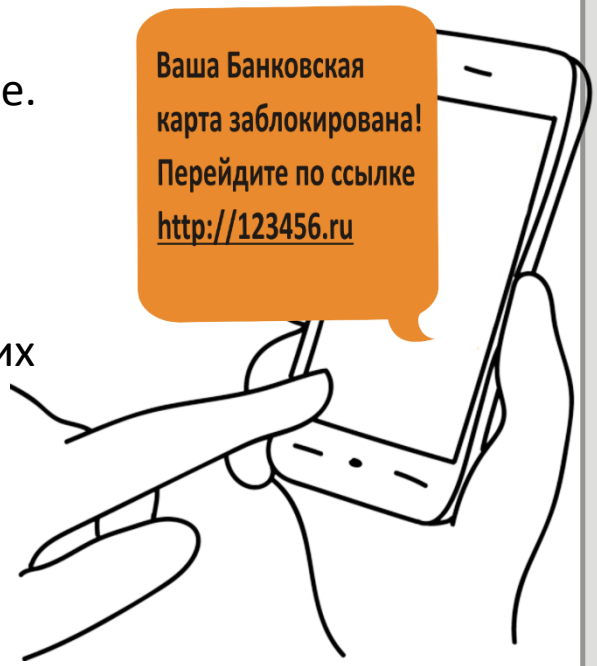
ФИШИНГ- ЭТО…

(англ. phishing от fishing «рыбная ловля, выуживание»)— вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.



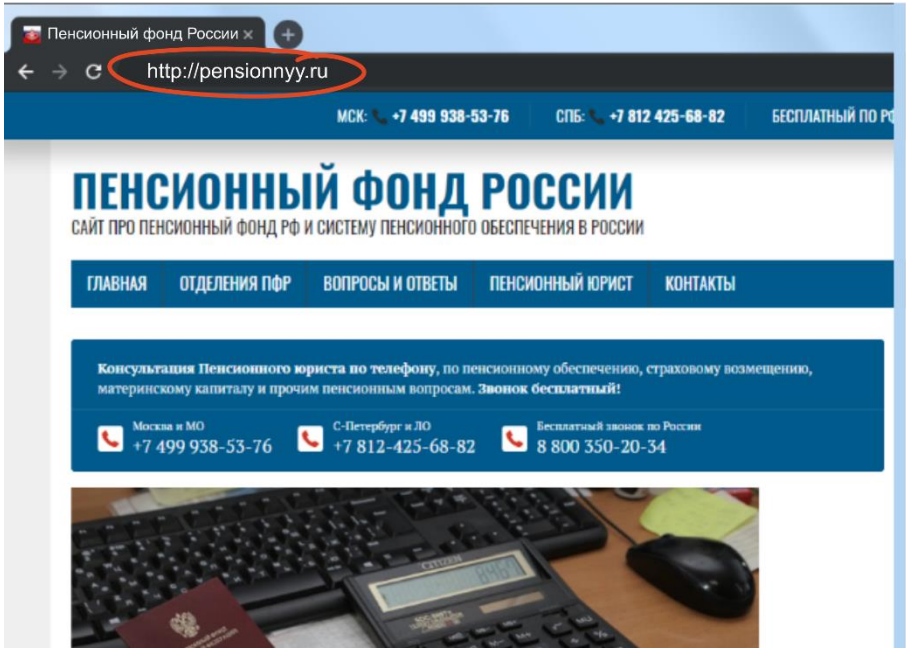
ПРИЗНАКИ ФИШИНГОВОГО САЙТА

- 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.

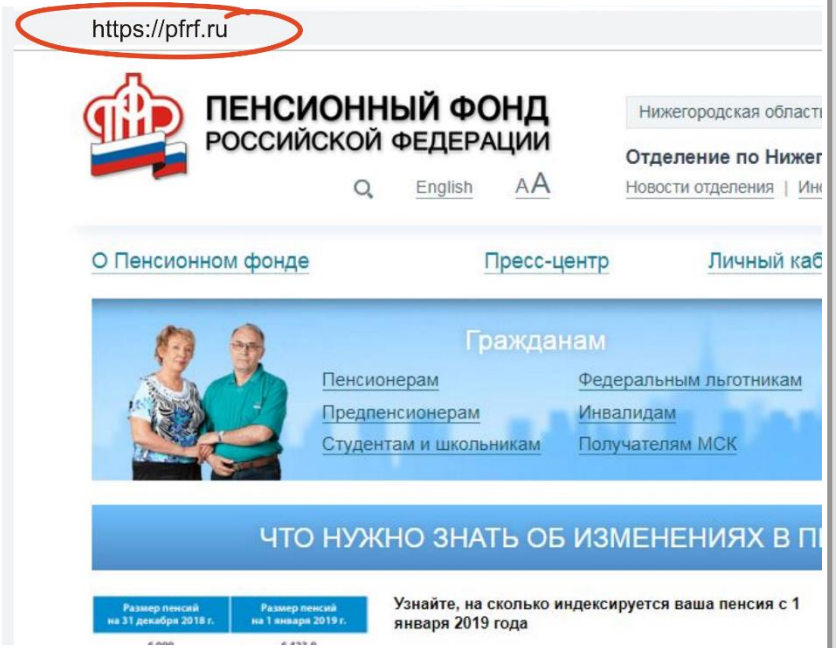


ПРИМЕР ФИШИНГОВОГО САЙТА

Фишинговый сайт



Хороший сайт

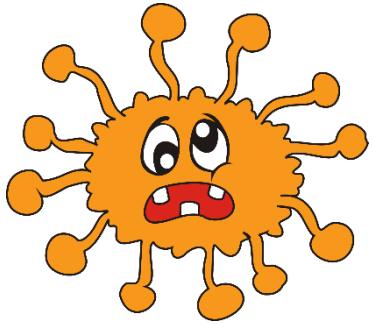


ТЕЛЕФОННЫЕ МОШЕННИКИ

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

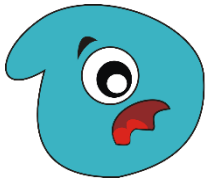
С МОЕЙ КАРТЫ СПИСАЛИ ДЕНЬГИ. ЧТО ДЕЛАТЬ?

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



Интерактив

Как не стать жертвой мошенников?



Напишите ответ в чат

СЕМЬ ПРАВИЛ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОЙ СРЕДЕ

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!!!

Банк России – мегарегулятор финансового рынка

Функции Банка России:

- Защита и обеспечение устойчивости рубля
- Поддержание стабильности и развития финансового рынка
- Защита прав потребителей финансовых услуг и повышение уровня финансовой грамотности населения

Узнайте больше о финансах:

Читайте статьи и новости:
fincult.info

Задавайте вопросы:
cbr.ru/Reception/

Звоните бесплатно:
8-800-300-3000

Для получения Сертификата участника

направляйте отзывы на **basewebinar@fincult.com**

Форму отзыва все участники получат
на электронную почту **в течение суток после урока.**

В случае возникновения вопросов, пожалуйста,
обращайтесь к нам **help@fincult.com**

Подписывайтесь в группы «Финансовое просвещение»!

Facebook: https://www.facebook.com/groups/finprosvet/

Одноклассники: https://ok.ru/finprosvet

ВКонтакте: https://vk.com/finprosv