

Банк России

**ПРАВИЛА ФИНАНСОВОЙ
БЕЗОПАСНОСТИ
В ВИРТУАЛЬНОЙ
СРЕДЕ**

ПРИ ИСПОЛЬЗОВАНИИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА НЕЛЬЗЯ:



Открывать подозрительные вложения.



Скачивать и устанавливать «пиратское» ПО.



Вставлять непроверенные флешки, смартфоны и др.



Сообщать личные данные, пароли и коды.



Работать без установки антивируса.

ЧТО ДЕЛАЕТ ЗАРАЖЕННЫЙ КОМПЬЮТЕР:

Похищает информацию.

Участвует в атаках.

Нарушает достоверность информации.



ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКИХ КАРТ НЕЛЬЗЯ:



Хранить данные карт на компьютере или в смартфоне.



Терять карту из вида (в магазине, кафе).



Передавать карту посторонним людям.



Сообщать секретный код из СМС при совершении покупок через интернет.



Пользоваться банкоматом, если он вызывает подозрения.



Сообщать данные вашей карты посторонним людям.



Использовать в местах, которые не заслуживают доверия.

КАК ОБЕЗОПАСИТЬ СЕБЯ?



Подключите мобильный банк и СМС-уведомления.

В случае любых проблем с картой срочно **свяжитесь** с банком и заблокируйте её.

Будьте внимательны.

ОСТОРОЖНО! ТЕЛЕФОННЫЕ МОШЕННИКИ!!!



СМС или письмо якобы от банка с просьбой перезвонить.



СМС об ошибочном зачислении средств или с просьбой подтвердить покупку.



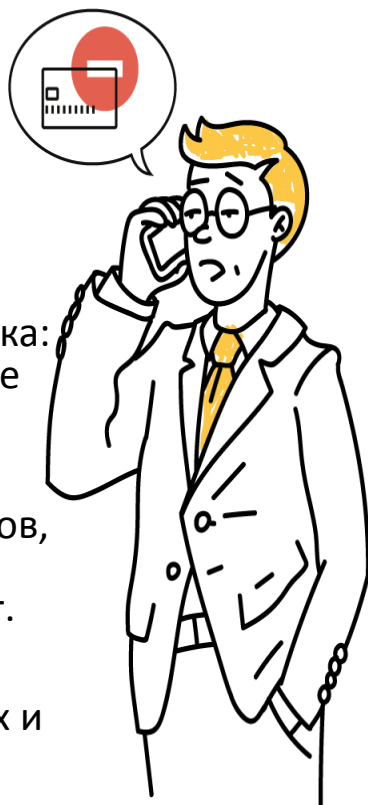
Звонок якобы от имени банка: вас просят сообщить личные данные.



СМС от имени родственников, которые просят перевести деньги на неизвестный счет.



Сообщения в мессенджерах и социальных сетях от неизвестных источников с просьбой о помощи или перечислить денежные средства на сомнительные счета, номера телефонов.



ПРИ ИСПОЛЬЗОВАНИИ ТЕЛЕФОНА НУЖНО:



Всегда **проверять** информацию.



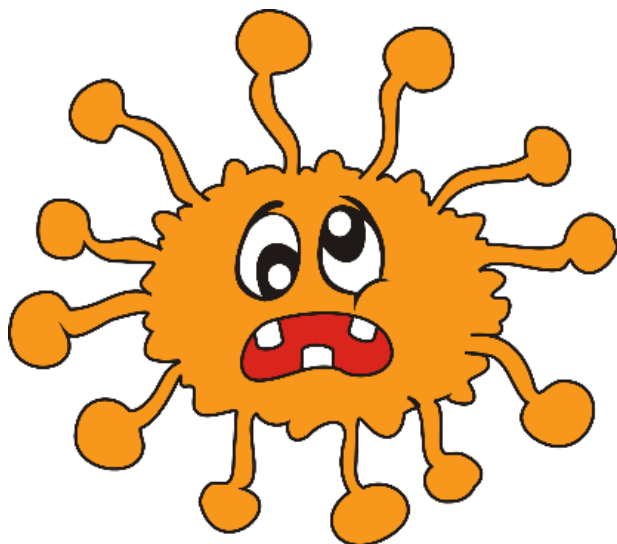
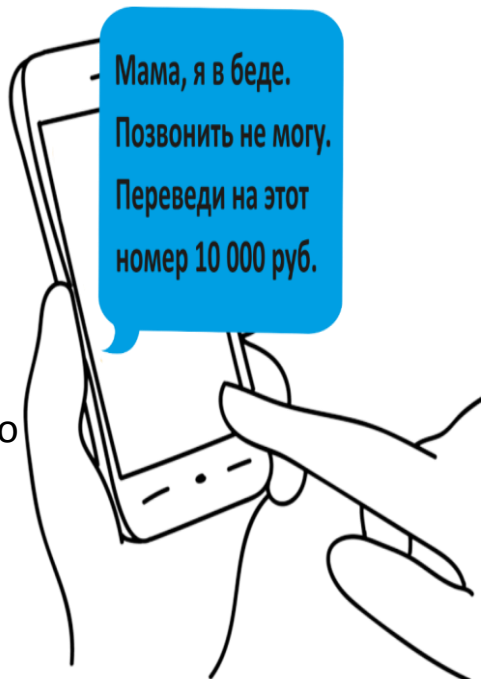
Не переходить по неизвестным ссылкам.



Если вам сообщают, что что-то случилось с родственниками, срочно **связаться** с ними напрямую.

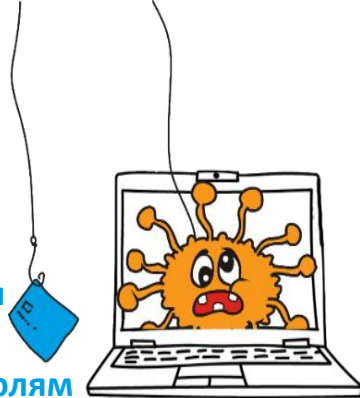


Не перезванивать по сомнительным номерам.



ОСТОРОЖНО! ФИШИНГ!!!

(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.



Есть опечатки, несоответствия, ошибки, небрежности.



На странице оплаты отсутствуют логотипы программ MasterCard SecureCode и Verified by Visa, использующих технологию 3D-Secure.

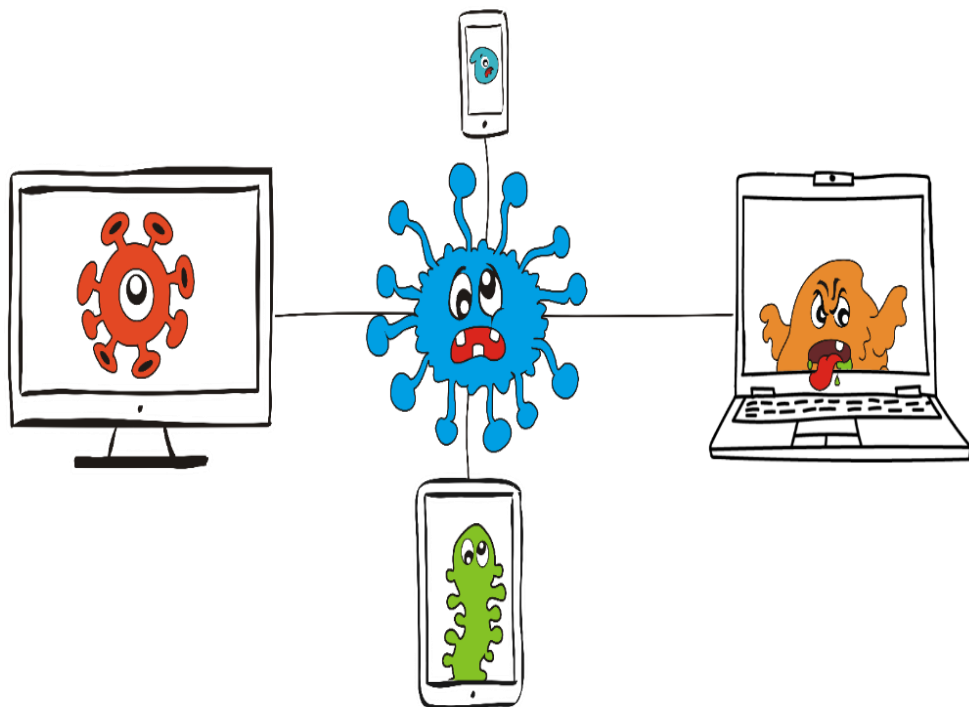


Ссылка пришла из неизвестного источника - СМС или социальные сети.



Вы попали на сайт при использовании открытой сети Wi-Fi без пароля.

**ЗАПОМНИТЕ ЭТИ ПРОСТЫЕ ПРАВИЛА И
БУДЬТЕ ОЧЕНЬ ВНИМАТЕЛЬНЫ!!!**



**ОБЪЯСНИТЕ ПОЖИЛЫМ ЛЮДЯМ,
РОДНЫМ И ДРУЗЬЯМ,
КАК НЕ СТАТЬ ЖЕРТВОЙ
МОШЕННИКОВ!!!**



**УЗНАЙТЕ БОЛЬШЕ НА
ИНФОРМАЦИОННО-
ПРОСВЕТИТЕЛЬСКОМ РЕСУРСЕ
БАНКА РОССИИ**

**«ФИНАНСОВАЯ КУЛЬТУРА»
FINCULT.INFO**

