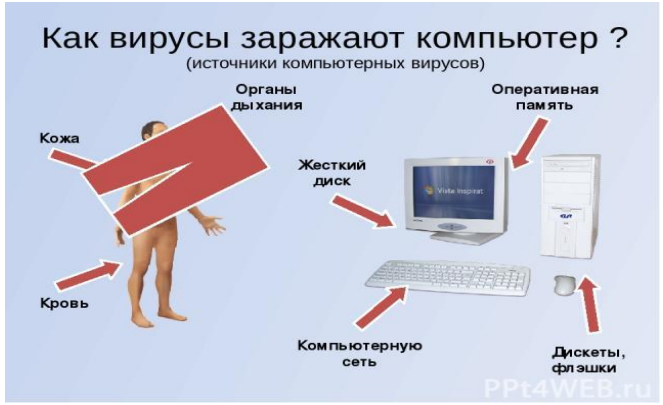
Еще одним высокотехнологичным способом хищения является вирусное заражение компьютеров и мобильных телефонов. Наиболее подвержены вирусной атаке клиенты банков, использующие СМС-банкинг и мобильные банковские приложения на таких устройствах.

Вирусы могут распространяться как через СМС, ММС-сообщения, так и через популярные мессенджеры, что резко снижает возможность их выявления со стороны операторов сотовой связи.

Преступления данного вида совершаются следующим образом, владелец смартфона получает сообщение, в тексте которого имеется ссылка, при открытии инициирующая загрузку вирусной программы. Как только вирус попадает в смартфон, он начинает рассылать СМС по контактным листам пользователя. Параллельно он делает запрос на номер СМС-банка и узнает баланс счета владельца смартфона. После этого вирусная программа переводит деньги на счета, подконтрольные злоумышленникам.




Вирус способен перехватывать входящие СМС-сообщения, поэтому владелец смартфона может не знать о снятии денег со счета, ведь оповещения о списаниях не доходят. В некоторых случаях вирус может блокировать смартфон.

С целью защиты электронных устройств от вирусных атак, необходимо обеспечивать их антивирусной защитой.

Таким образом, если раньше преступникам требовалось получить физический доступ к деньгам жертвы, то теперь достаточно получить доступ к конфиденциальной информации. Именно при помощи такой информации, которую граждане зачастую сами охотно сообщают аферистам, последним удается удаленным способом похитить любые суммы денежных средств, вывести их на любые выбранные ими счета и обналичить в любой точке мира. Реагировать на подобные звонки и сообщения следует спокойно и рассудительно, не поддаваться на уговоры, обязательно проверить информацию.

Если вам сообщили о блокировке карты, необходимо обратиться в ближайшее отделение банка, либо по телефону, указанному на банковской карте.

Если вам сообщили о том, что кто-то из родственников попал в неприятности, необходимо задать контрольный вопрос, ответ на который знаете только вы и родственник, а лучше всего дозвониться до последнего.

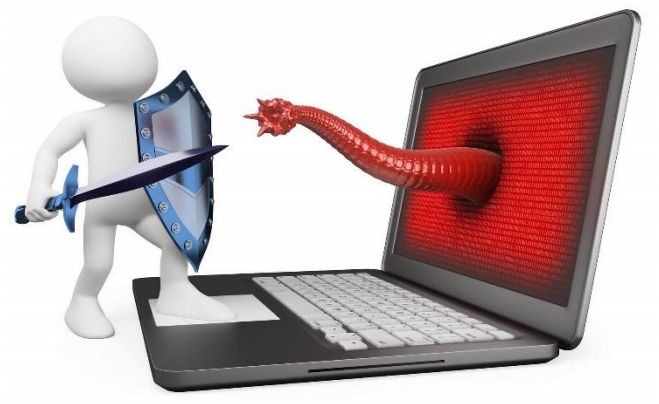
Ни в коем случае нельзя сообщать по телефону информацию, касающуюся банковской карты, персональных данных и наличие на ней денежных средств.

При дистанционном общении важно учитывать, что, если с вас требуют предоплату для выполнения условий договора купли-продажи, устройства на работу, получения выигрыша, в отношении вас совершаются противоправные действия.

При смене СИМ-карты не забывайте отключать мобильный банк. Если вы заподозрили, что перевели деньги злоумышленникам, то следует немедленно отменять операцию.

Важно понимать, что сохранность ваших сбережений в большей степени зависит от вас, будьте бдительны, проверяйте информацию любым доступным для вас способом.

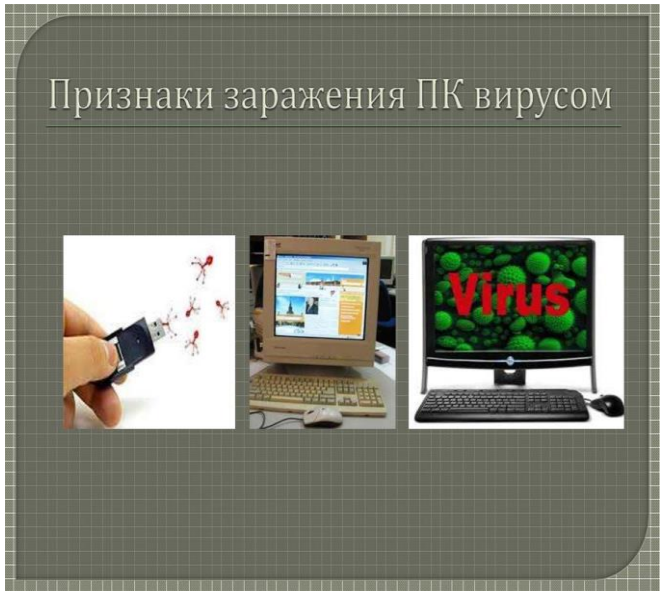
Поэтому, если вам позвонили или прислали СМС подозрительного содержания, либо вы наткнулись на мошенническое объявление, обязательно сообщите об этом в полицию.



33780, Краснодарский край,
Калининский район, ст. Калининская,
ул. Фадеева, 147
email:cso_otrada@mtsr.krasnodar.ru
Исполняющий обязанности
директора Масенко С.Н.
Тел.:24-4-52

Министерство труда и социального развития Краснодарского края
ГБУ СО КК «Калининский КЦСОН»

# Информация для населения о вирусное заражение компьютеров и мобильных телефонов




*ст. Калининская*
*2024 год*