

Существуют общие правила поведения с кибермошенниками.

Следуя им, вы сможете себя обезопасить:

– не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;



– установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

Остерегайтесь мошенников!



звонят с похожих номеров банка



представляются сотрудниками банка



говорят, что кто-то пытается украсть ваши средства



спрашивают или просят ввести данные карты и коды из SMS

Чтобы защититься от мошенников



не сообщайте посторонним коды из SMS, номер карты, срок действия, ПИН-код, CVC/CVC и логин/пароль для Smartbank



не меняйте номер телефона для Smartbank по чьей-либо просьбе



не открывайте письма от подозрительных адресатов



не переходите по ссылкам, полученным из сомнительного источника

– не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреватые как минимум списанием значительной суммы с вашего мобильного счета, а как максимум – быть поводом для мошенников активизировать против вас мошенническую схему;

– не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;

– заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получают доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

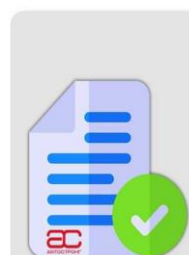
ВНИМАНИЕ!
ОПАСАЙТЕСЬ МОШЕННИКОВ



Не доверяйте непроверенным продавцам запчастей



Не передавайте деньги, не убедившись, что это не фейк



Покупайте запчасти у проверенных компаний

В случае если вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, – вы рискуете попасть на мошенников. Чтобы связаться с банком, самостоятельно наберите номер, указанный на обратной стороне вашей банковской карты или на официальном сайте кредитной организации.

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ



Для того чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также

подтверждающий код из СМС) – это, как правило, бесплатно. Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (Яндекс, Mail.ru), помеченными цветным кружком с галочкой.

МВД УДМУРТИИ ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!

МОШЕННИКИ!

Звонок от «сотрудника банка»

ПРИЗНАКИ

- 1 поступление звонка от «сотрудника банка» (специалиста, работника службы безопасности);
- 2 сообщение о попытке хищения денежных средств; предложение заблокировать несанкционированную операцию либо перевести денежные средства на «безопасный» счет;
- 3 просьба назвать реквизиты банковской карты, защитный код с ее обратной стороны и поступающие на телефон пароли.

33780, Краснодарский край,
Калининский район, ст. Калининская,
ул. Фадеева, 147
email: cso_otrada@mtsr.krasnodar.ru
Директор О.В. Коротенко
Тел.: 24-4-52

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

Общие правила поведения с кибермошенниками

Кибермошенничество

С момента изобретения интернета добраться до подростков стало намного легче, используя наивность и неопытность.

- ✓ Просьба ввести свой реальный номер телефона, чтобы выяснить, что вы не робот, затем ...
- ✓ на телефон приходят SMS сообщения о розыгрыше автомобиля, выигрыше в лотереи....
- ✓ для участия надо отправить в ответ сообщение с текстом «я счастливчик», итогом такой операции будет снятие денег с мобильного счета.

ст. Калининская
2023 год