Бдительность рубль бережёт!

Мишенью для мошенников может стать любой, а вот если у этого человека есть деньги и недостаточно бдительности, чтобы защититься от хитроумных злоумышленников, он очень быстро превращается в жертву.

В последние годы все больше от действий кибермошенников страдают куряне, имеющие электронные аккаунты и почтовые ящики. В зоне риска каждый, поскольку мошенники автоматизируют большинство своих атак.

Специалисты регионального отделения Банка России напомнили курянам несколько основных правил, следуя которым можно обезопасить себя от финансовых потерь.

Надежные пароли

Это очень важно! Пароль должен состоять из сложного сочетания символов. При этом для каждого отдельного сервиса и сайта он должен быть свой. Нельзя сообщать кому-то свои пароли, хранить их записанными на бумаге, вводить на сторонних сайтах.

Конфиденциальность

Если вам нужно оставить свой компьютер, телефон или планшет на какое-то время — независимо от того, как быстро вы вернетесь — заблокируйте его, чтобы никто не мог воспользоваться им, пока вас нет. Не давайте возможности недоброжелателям легко получить доступ к вашей конфиденциальной информации.

Безопасность при совершении платежных операций.

Не заходите в онлайн-банкинг и не совершайте покупки онлайн с чужих устройств или из общественных сетей, чтобы ваши банковские данные не смогли собрать и украсть киберпреступники.

Антивирус

Он поможет вовремя выявить вредоносные программы и защитить компьютер от возможных угроз. Антивирус нужно установить на смартфон или планшет, особенно если эти устройства используются для осуществления платежей.

Резервное копирование данных

Поможет не только в случае системного сбоя на устройстве, но и в при поражении компьютера вирусом-шифровальщиком. Чтобы не потерять важную информацию, нужно время от времени повторять резервное копирование данных.

Известные накопители

Никогда не подключайтесь к USB-накопителю или устройству, происхождение которого неизвестно. Они могут быть заражены вредоносными программами.

Двухфакторная аутентификация

Чем больше уровней защиты используется, тем увереннее можно быть в том, что с устройствами и данными ничего не случится. Активируйте двухфакторную аутентификацию на всех аккаунтах, где это возможно.

Проверка банковской отчетности

Историю платежей следует проверять регулярно. Эту возможность дает онлайн-банкинг. Отслеживайте подозрительную активность и при необходимости сразу уведомите свой банк, смените пароль и убедитесь, что применили все доступные меры безопасности.

Только проверенные ссылки и баннеры

Обращайте внимание на написание URL-адреса. Адресная строка должна начинаться с https://, в строке должен быть знак закрытого замочка – это значит, что соединение защищено. Обращайте на это особое внимание, когда переходите на страницу оплаты, где надо ввести данные банковской карты. Запомните: фишинговые сайты часто имитируют интерфейсы банков и онлайн-магазинов, заменяя лишь один или несколько символов в ссылке. Кроме того, вредоносные домены часто содержат сложные комбинации символов или орфографические ошибки.

Спаму – нет!

Сообщайте свой адрес электронной почты только тем людям и компаниям, которым вы доверяете. Не заполняйте ненужные формы, где просят указать e-mail. Если вы получили спам, отметьте его, чтобы помочь вашему провайдеру электронной почты более эффективно блокировать спам в дальнейшем.