# Как обезопасить себя в век информационных технологий



В современном мире информационных технологий возможности сети Интернет широко используются в повседневной жизни. Однако, помимо огромного количества полезных возможностей сеть Интернет несёт в себе и определённую опасность. В связи с этим, немаловажным является предупредить пользователей глобальной сети о том, какую именно опасность может нести «всемирная паутина» и какие действия нужно предпринимать, чтобы общение посредством Интернет оставило только положительные эмоции.

Так, отмечается рост случаев обращений о совершении в отношении граждан мошеннических действий. Все больше потребителей совершают покупки онлайн, расплачиваются картой и меньше пользуются банкоматом. При этом появляются новые схемы мошенничества, которые не требуют особой квалификации или вложений средств.

© 2024 Следственное управление Следственного комитета Российской Федерации по Тверской области

Чтобы не стать жертвой мошенников необходимо соблюдать правила цифровой или компьютерной гигиены, сохранять бдительность, использовать сложные и разные пароли. При каждой оплате товаров или услуг с помощью электронных средств платежа необходимо помнить следующие правила: не использовать подозрительные Интернет-сайты, подключить Интернет-банк и СМС-оповещение, не сообщать данные своей карты другим людям, в том числе банковским служащим, работникам интернет-магазинов, при возможности открыть отдельную карту, на которой хранить определенную сумму денежных средств для осуществления безналичных платежей. Важно помнить и о соблюдении ряда основных правил работы в сети Интернет и, в частности, в социальных сетях. Важно знать, что информация, размещённая гражданами в социальных сетях, может быть найдена и использована кем угодно.

Основная задача граждан при принятии решения о приобретении товара через Интернет-магазин, поступлении посредством сотовой связи просьбы об оказании помощи в связи с непредвиденными обстоятельствами, сложившимися с их родственниками, быть осмотрительными и проверить доступным способом поступающую информацию, прежде чем перечислять денежные средства в адрес злоумышленников.

Возросло количество «телефонного мошенничества» с использованием абонентских номеров правоохранительных органов. В разговорах с гражданами мошенники, представляясь сотрудниками силовых ведомств, склоняют жителей региона к действиям, приводящим к утрате личных денежных средств. Такие действия квалифицируются как «мошенничество».

Обращаем внимание граждан:

- сотрудники правоохранительных органов, уполномоченные проводить предварительное следствие, вызывают граждан повесткой. При этом должностное лицо никогда не требует по телефону предоставления персональных данных, банковских реквизитов, информации по счетам и пластиковым картам;

- ни по телефону, ни в ходе очной беседы сотрудники правоохранительных органов не заявляют требований о переводе денежных средств на какие-либо счета. Это незаконно;

© 2024 Следственное управление Следственного комитета Российской Федерации по Тверской области

- желая проверить мошенников, не следует перезванивать на такие входящие вызовы;

- любые предложения от имени правоохранительных органов, например, помочь в поимке преступника путем перечисления денег на указанные «собеседником» счета либо с целью обезопасить сбережения – это явный признак мошенничества. О таких фактах необходимо сразу сообщить в правоохранительные органы;

- при попадании в подобные ситуации (если звонящий представился сотрудником силовых структур) необходимо позвонить по номерам телефона доверия соответствующего правоохранительного органа и проверить информацию, озвученную звонившим.

С целью профилактики заражения компьютера вирусами и вредоносным программным обеспечением необходимо знать о правилах компьютерной гигиены, следование которым поможет минимизировать вероятность поражения компьютера, а именно:

1) Приобретите и пользуйтесь платным антивирусом. Отсутствие антивируса резко увеличивает вероятность заражения компьютера, а бесплатные продукты обычно имеют сильно урезанный функционал.

2) Используйте антивирус. Зачастую, установив на компьютер новейший навороченный продукт от известной компании, пользователь забывает о его существовании. Между тем, простой установки антивируса бывает недостаточно для эффективного противостояния угрозам.

За мошенничество с использованием электронных средств предусмотрена уголовная ответственность. Так, уголовная ответственность предусмотрена по статье 159.3 Уголовного кодекса за мошенничество с использованием электронных средств платежа.

Также предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (статья 159.6 Уголовного кодекса РФ).

© 2024 Следственное управление Следственного комитета Российской Федерации по Тверской области

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошеннических действий, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы.

*22 Января 2023*

*Адрес страницы:* https://tver.sledcom.ru/news/item/1759985

© 2024 Следственное управление Следственного комитета Российской Федерации по Тверской области