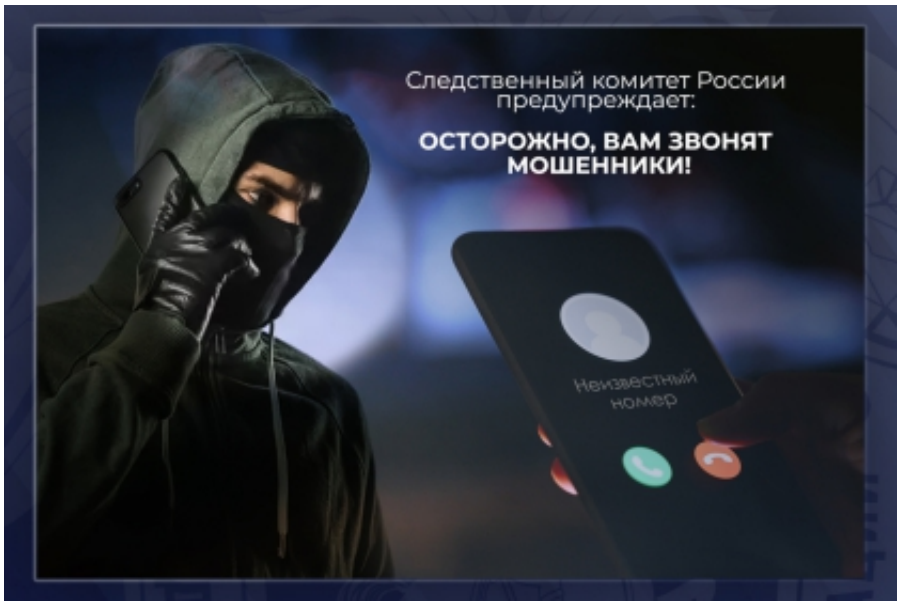
Следственный комитет обращает внимание граждан на защиту от мошенников в сфере компьютерной информации



В нашей повседневной жизни используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, банковскими картами и компьютерами, то есть знать правила «компьютерной гигиены».

Одной из распространенных форм компьютерного мошенничества связано с использованием телефонных вирусов. Например, на телефон абонента приходит сообщение вида: «Вам пришло сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

В последнее время наблюдается рост числа случаев мошенничества с банковскими картами и поэтому необходимо следовать элементарным правилам цифровой безопасности:

- Никогда и никому не сообщайте ПИН-код Вашей карты.

- Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

- Ни у кого нет прав требовать ваш Пин-код. Хранение реквизитов и ПИН-кода в тайне – это ваша ответственность и обязанность.

- Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

- Совершая операции с банковской картой, следите, чтобы рядом не было посторонних людей.

- Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств вы сняли, и какие цифры вводили в банкомат, могут быть использованы мошенниками.

Как защититься от мошенников в Интернете? «Компьютерная гигиена» предусматривает защиту от доступа вредоносных программ к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом «вирусы». На самом деле вредоносные программы можно разделить на три группы:

- компьютерные вирусы;

- сетевые «черви»;

- троянские программы.

Компьютерные вирусы – это программы, которые умеют размножаться и внедрять свои копии в другие программы, то есть заражать уже существующие файлы.

Сетевые «черви» могут распространяться по локальным сетям и Интернету (например, через электронную почту). Червь без Вашего ведома может, например, отправить «червивые» сообщения всем респондентам, адреса которых имеются в адресной книге Вашей почтовой программы. Помимо загрузки сети в результате лавинообразного распространения, сетевые «черви» способны выполнять опасные действия.

Задача троянской программы – обеспечить злоумышленнику доступ к Вашему компьютеру и

возможность управления им. Может случиться так, что однажды ваша частная переписка будет опубликована в Интернете или баланс в ваших электронных платежных системах неожиданно окажется нулевым или отрицательным.

Для защиты от вредоносных программ пользователю персональным компьютером необходимо установить антивирусное программное обеспечение и регулярно обновлять антивирусные программы.

- Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте.

- Подозрительные файлы лучше немедленно удалять.

- Проверяйте все новые файлы, сохраняемые на компьютере.

- По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

- При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

Статистика показывает, что преступлений, связанных с мошенничеством в сфере компьютерной информации, становится с каждым годом все больше, и пользователи сети Интернет зачастую становятся потерпевшими из-за собственной беспечности и незнания правил «компьютерной гигиены».

Законодательством Российской Федерации предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации (159.6 УК РФ) и мошенничество с использованием электронных средств платежа (159.3 УК РФ). За преступления, связанные с указанными видами мошеннических действий, в зависимости от их тяжести предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишение свободы.

24 Августа 2023

Адрес страницы: https://osetia.sledcom.ru/news/item/1818877