Из рубрики: Кибербезопасность

На сегодняшний день с развитием интернета и IT-технологий подвергнуться атаке преступников можно даже не выходя из дома

Наиболее распространенные виды кибермошенничества:

«Вишинг» - завладение данными клиента по телефону. Вам звонят и представляются сотрудниками милиции, банков или других служб, с целью узнать личную информацию по картам или обманом вынудить Вас перевести деньги мошенникам.

Будьте бдительны! Сотрудники финансовых учреждений никогда не требуют предоставить им по телефону конфиденциальную информацию о банковской карте или счете.

«Фишинг» - мошенничество, построенное на получении информации о вашей карте путем рассылки электронных писем со ссылками, ведущими на подозрительный сайт. На этом сайте пользователю будет предложено сообщить пин-код карты, cvv/cvc-код и СМС-коды, полученные от банка.

Будьте внимательны! Проверяйте ссылку, которая стоит в адресной строке или посмотрите в опции «свойства ссылки», на какой сайт она ведёт.

«Фарминг» - перенаправление пользователей на поддельные сайты с помощью вредоносный кода, который устанавливается на компьютер или сервер жертвы. Там предлагается ввести персональную информацию, которая может быть использована в мошеннических целях.

Установите на личный компьютер, планшет, смартфон, телефон лицензионную антивирусную программу, которая своевременно сможет распознать незаконное вмешательство в устройства.

«Скимминг» - схема, при которой преступники копируют магнитную полосу карты и считывают ее пин-код с помощью устройства, прикрепленного к банкомату. На основании полученных данных - изготавливают поддельную карту и снимают деньги.

Пользуйтесь только теми банкоматами, которые установлены в госучреждениях, банках, торговых центрах.

Поделитесь информацией с вашими родными и близкими, а также пожилыми родственниками и знакомыми.
