КАК ОБЕЗОПАСИТЬ СЕБЯ И СВОИ ДЕНЕЖНЫЕ СРЕДСТВА ОТ ХИЩЕНИЙ В СЕТИ ИНТЕРНЕТ

Для того, что бы обезопасить себя и свои денежные средства от хищений в сети Интернет необходимо:

1. Исключить передачу данных своей банковской пластиковой карты (далее - БПК) третьим лицам каким бы то ни было способом, так как участились случаи взломов страниц в социальных сетях, а также не реагировать на поступающие рассылки с просьбой о помощи переводов, оплаты либо снятии денежных средств при помощи вашей БПК.

2. В случае обнаружения утери, либо передачи данных карты немедленно связаться с банком-эмитентом карты, сообщить об утере и заблокировать доступ с помощью указанной карты к банковскому счету (для возможности экстренной блокировки банковской карты необходимо всегда дополнительно иметь при себе контактные телефоны банка, которые для сведения указаны на оборотной стороне БПК).

3. В ходе использования БПК подключить и использовать технологию «3D Secure». На настоящий момент это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. Позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию по переводу денежных средств, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель БПК подтверждает каждую операцию по своей карте специальным одноразовым уникальным кодом, который получает в виде СМС-сообщения на свой номер мобильного телефона.

Кроме того, следует помнить, что в случае обнаружения утерянной кем-либо БПК не стоит выкладывать ее фотографии в сети Интернет с целью поиска владельца. Информации, содержащейся на изображении карты с лицевой стороны, достаточно для совершения операций с использованием карты без ведома владельца БПК, чем и пользуются злоумышленники.

Материалы предоставлены
Дрибинским Районным отделом Следственного комитета

КАК ОБЕЗОПАСИТЬ СЕБЯ И СВОЮ СТРАНИЦУ В СОЦИАЛЬНОЙ СЕТИ «ВКонтакте» ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

1. Защитить свою страницу сложным паролем. Пароль от электронной почты, с помощью которой зарегистрирован аккаунт, также должен быть сложным и не должен совпадать с паролем от Вашего аккаунта. Старайтесь менять пароль от личной страницы «ВКонтакте» не реже одного раза в три месяца.

2. Не устанавливать сомнительные приложения и программы на свои мобильные телефоны, персональные компьютеры и иные устройства.

Как правило, кражу паролей злоумышленники маскируют под какой-нибудь «приват» или «чат». Запомните простое правило: работая в приложениях, либо на страницах в социальных сетях вы уже находитесь в авторизованном статусе.

3. Не переходите по сомнительным ссылкам. Фишинг - это распространенный вид мошенничества, который осуществляется путем подставных страниц. Подставная страница - это страница того или иного Интернет-ресурса, где вы проходите авторизацию, во время которой вам требуется ввести свой логин и пароль. На внешний вид она практически не отличается от оригинальной. Например, «фейковая» страница в социальной сети «Вконтакте» может быть полной копией официальной страницы, но с одним отличием, незаметным большинству пользователей сетевым адресом, типа https://vk.ru/ и т.п.

4. Используйте на устройствах современное (лицензионное) антивирусное программное обеспечение с актуальными базами.

5. Настройте двукратную авторизацию. Для активации данной функции войдите в меню «Мои настройки». Вкладка «Общие», «Безопасность вашей страницы», где напротив пункта «Подтверждение входа» следует нажать «подключить». Это активирует дополнительный уровень проверки, при котором знание вашего логина и пароля будет уже недостаточно. Теперь для успешной авторизации необходимо ввести специальный код подтверждения. Получить специальный код подтверждения можно как с помощью бесплатного SMS на номер привязанного к странице телефона, так и с помощью специального приложения для смартфона. При авторизации вы можете запомнить данный браузер, далее для входа с него будет достаточно ввести логин и пароль, код больше не потребуется. Если кто-то попытается зайти на вашу страницу, вы получите всплывающее сообщение.

При соблюдении всех правил (причем одновременном) вы можете быть уверены, что никто кроме вас не получит доступ к аккаунту, и, соответственно, гарантируете себе надежную защиту личной страницы «ВКонтакте» от взлома.

Материалы предоставлены
Дрибинским Районным отделом Следственного комитета