Новости

Общество

30.08.2024

«Осторожно мошенники!»: как обеспечить себе информационную безопасность в сети

Сегодня в Беларуси уделяется повышенное внимание обеспечению защищенности информационного пространства. Анализ материалов уголовных дел анализируемой категории свидетельствует о незнании потерпевшими элементарных мер по обеспечению безопасности своего карт-счета. Большинство хищений денежных средств с банковских счетов, доступ к которым обеспечивается при использовании банковских платежных карт совершаются после того, как потерпевшие сами сообщали необходимые реквизиты своих банковских карточек.

Управление Фрунзенского районного отдела Следственного комитета Республики Беларусь напоминает о мерах профилактики преступлений против информационной безопасности, а также о хищениях с использованием компьютерной техники:

1. Не разглашать логины, финансовые номера телефонов пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW-коды, данные касательно последних платежей и срока действия пластиковых карт третьим лицам;

2. В ходе использования карты 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, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель банковской карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на

свой мобильный телефон;

3. Исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, каким бы то ни было способом;

4. Вводить секретные данные только на сайтах, защищённых сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://;>;

5. Производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

6. Не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации);

7. Подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2-4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга;

8. Не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт пользуется общественный компьютер;

9. В ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утили;

10. Вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адресу. Это действие обеспечит максимальный уровень безопасности;

11. В целях предотвращения хищений денежных средств абонента сотовой связи через мобильный банкинг не следует передавать телефон другим лицам, а также необходимо установить на мобильном телефоне блокировку (с помощью пароля, сканера отпечатка пальца, фейсконтроля и т.п.).

Будьте внимательны, берегите себя и свои персональные данные!