Знайте правила, чтобы не стать жертвой киберпреступлений

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники. В Республике Беларусь отмечается ежегодный рост преступлений, связанных с хищением денежных средств организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.
Подавляющее большинство данных преступлений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет). Технология основана на использовании слабостей человеческого фактора и является достаточно эффективной. Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке. Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступник, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной сумму денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации.
Так называемый фишинг-тоже техника «социальной инженерии», направленная на получение конфиденциальной информации. Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо–от банка или платежной системы–требующее «проверки» определенной информации, или совершения определенных действий. Это письмо, как правило, содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.
Правила, которые помогут Вам не стать жертвой киберпреступлений:

* храните номер карточки и ПИН-коды в тайне;
* не используйте один пароль для всех интернет-ресурсов;
* поставьте лимит на сумму списаний или перевода в личном кабинете банка;
* не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;
* не переводите денежные средства на счета незнакомых лиц;
* не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты;
* не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
* не размещайте в открытом доступе и не передавайте информацию личного характера.

**Отделение уголовного розыска Октябрьского РОВД.**