Тезисы
по теме «Профилактики преступлений и правонарушений в сфере высоких технологий»

Правила «цифровой» гигиены:

Наряду с традиционными «бумажными» деньгами сейчас появились иные способы оплаты, и все они так или иначе связаны с компьютерами. Как не стать ЖЕРТВОЙ преступления и не потерять свои деньги? Такие правила называют «цифровой гигиеной».

1) БАНКОВСКИЕ ПЛАТЕЖНЫЕ КАРТОЧКИ (БПК) – представляют собой пластиковую карточку снабженную магнитной полосой, а в современных БПК и чипом (миниатюрным компьютером), на которых записан код, позволяющий получить через различные устройства (банковские терминалы, банкоматы, инфо-киоски) доступ к вашему счету в банке. Получив такой доступ, можно производить оплату, брать кредит и пользоваться другими услугами банка. Современные БПК снабжены поддерживают беспроводные соединения
Правом такого доступа обладает владелец карты. Доступ, осуществленный посторонним без разрешения владельца БПК называется НЕСАНКЦИОНИРОВАННЫМ.
Чтобы обезопасить владельца БПК от несанкционированного доступа существуют ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ:
- ПИН-КОД – 4 цифры, которые надо вводить при расчете картой через банкомат либо терминал;
- код CVV/CVC – 3 цифры на обратной стороне карты, которые нужны при расчетах карточкой через сеть Интернет;
- 3D-SECURE/SECURECODE - подтверждение операций с БПК в сети Интернет посредством ввода кода, который приходит по СМС на номер мобильного телефона.

Любые платежные операции, совершенные без разрешения владельца в ходе несанкционированного доступа преследуются по закону в порядке статьи 212 «Хищение с использованием компьютерной техники» уголовного кодека Республики Беларусь. При этом не важно сколько денег похищено – 1000 рублей или 1, в таких действиях есть состав преступления.

При пользовании БПК необходимо соблюдать простые правила:

- ни под каким предлогом никому не сообщать ПИН-КОД банковской платежной карты и код CVV/CVC. Для зачисления денег вам на карточку, достаточно сообщить ее номер и дату окончания действия. Попытка выяснения пин-кода либо кода CVV/CVC сигнализирует о том, что с вами общается МОШЕННИК. Не записывать пин-код на самой карте, ведь при ее утере вы лишитесь и всех денег;
- при получении банковской платежной карточки ОБЯЗАТЕЛЬНО использовать все доступные способы защиты, предлагаемые банками (двухфакторная авторизация, СМС-оповещение о расходных операциях, лимит снятия денежных средств и др.), ни в коем случае не сообщать содержимое таких СМС посторонним лицам;
- не передавать свою банковскую платежную карточку посторонним лицам. Помните злоумышленник может сфотографировать ее номер и код на обратной стороне, и использовать потом эти реквизиты для оплаты в сети Интернет;
- не открывать счета в банках в интересах третьих лиц и передавать реквизиты доступа к таким счетам за материальное вознаграждение. Помните, такие счета используются злоумышленниками для вывода похищенных денег!

2) МОБИЛЬНЫЙ ТЕЛЕФОН также может являться полноценным платежным средством. Используя счет мобильного телефона можно расплатиться за услуги в сети Интернет, либо открыть V-BANKING (когда ваш телефонный счет используется для расчетов, подобно банковской платежной карте). Для расчетов необходимо ввести номер мобильного телефона и код, полученный в СМС-сообщении. К мобильному телефону можно привязать БПК и использовать его для расчетов как банковскую платежную карточку.

Поэтому:

- при общении с посторонними лицами ни в коем случае не сообщать содержимое СМС-сообщений, приходящих вам на телефон и содержащий код – возможно ВАШ ТЕЛЕФОННЫЙ НОМЕР хотят использовать для оплаты;
- при добавлении БПК в программы, используемые на мобильном телефоне или компьютере следует помнить, что оплата по таким привязанным картам может происходить автоматически (например при окончании пробного бесплатного периода для программы, оплата за следующий период может происходить автоматически).

3) ИНТЕРНЕТ-БАНКИНГ представляет собой доступ к управлению счетом БПК через сеть Интернет.

Доступ к интернет-банкингу осуществляется через ввод имени пользователя и пароля. Для разрешения проведения платежных операций часто требуется ввод специального кода, который предоставляется на карточке банком, либо приходит в СМС сообщении на мобильный телефон.

Зачастую преступники, чтобы узнать имя пользователя и пароль к интернет-банкингу используют поддельные сайты в сети Интернет, имитирующие вид настоящего сайта, однако расположенные по другому адресу (фишинговые сайты, от англ. fishing - рыбалка). Как пример ФИШИНГОВЫЙ сайт ibank-belapb.ru. Так же реквизиты доступа могут похищаться программами-вирусами, в случае если ваш компьютер заражен.

Для того, чтобы обезопасить себя при работе с Интернет-банкингом необходимо:

- ни под каким предлогом НЕ СООБЩАТЬ постороннему лицу реквизиты доступа к Интернет-банкингу, такие как имя пользователя и пароль;
- использовать СЛОЖНЫЕ пароли доступа к системе «ИНТЕРНЕТ-БАНКИНГ», состоящие из цифр и букв. Не стоит в качестве пароля указывать дату рождения либо номер телефона. Такие пароли могут быть легко подобраны специальными программами. Не стоит использовать одинаковые пароли к электронной почте, интернет-банкингу и анкетам в социальных сетях;
- никому не сообщать ни под каким предлогом дополнительные коды, приходящие в СМС или полученные от сотрудников банка на карточке;
- не вводить реквизиты доступа к Интернет-банкингу внимательно не убедившись, что в адресной строке написан верный адрес сайта Интернет-банкинга. Кроме этого если сайт Интернет-банкинга не работает по защищенному протоколу HTTPS, так же не следует вводить реквизиты доступа, так как они могут быть перехвачены;
- использовать антивирусное программное обеспечение, которое регулярно обновляется.

4) Сеть ИНТЕРНЕТ.
Следует помнить, что кажущаяся анонимность пользователей сети Интернет провоцирует на совершение мошенничеств. Чтобы не потерять свои деньги следует выполнять простые правила:

- не обращать внимание на письма, полученные по электронной почты и содержащие информацию о выигрыше либо получении наследства (распространенная мошенническая схема, носящее название «Нигерийские письма»), добавлять такие письма в СПАМ;
- обращать внимание на адрес электронной почты, с которого поступило электронное письмо. Не открывать и не запускать вложения в электронных письмах, полученных от неизвестного отправителя;
- не переходить по неизвестным ссылкам, особенно если их подписи сулят вам выигрыш либо материальную выгоду;
- не соглашаться на установку предложенных неизвестными сайтами программ, особенно если это АНТИВИРУСЫ и другие программы по безопасности;
- не устанавливать программы, загруженные из неизвестных источников, они могут содержать ТРОЯНСКИЕ ПРОГРАММЫ ;
- не использовать неизвестные мобильные приложения, в которых требуется ввод платежных реквизитов, учетных данных аккаунтов электронной почты, интернет-банкинга, социальных сетей или иных интернет-ресурсов;
- не использовать сайты казино и брокерских контор, зарегистрированных за пределами Республики Беларусь, так как они в основном зарегистрированы в офшорных зонах и при возникновении финансовых споров, с большой долей вероятности вы не сможете вернуть свои деньги.