ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

ПО ИНФОРМАЦИИ ОТДЕЛА ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ УВД МОГИЛЕВСКОГО ОБЛИСПОЛКОМА В ТЕКУЩЕМ ГОДУ БЕЛОРУССКИЕ ПОЛЬЗОВАТЕЛИ СОЦИАЛЬНОЙ СЕТИ «ВКОНТАКТЕ» ВСЕ ЧАЩЕ СТАНОВЯТСЯ ЖЕРТВАМИ МОШЕННИЧЕСТВА И ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ.

Злоумышленники осуществляют несанкционированный доступ к личным страницам граждан и от их имени рассылают сообщения виртуальным друзьям. В них мошенники просят о помощи в получении денежного перевода и просят предоставить реквизиты банковской платежной карты (номер карты, срок действия и CVV-код).

CVV-код – это трехзначный код для проверки подлинности Вашей карты при оплате через Интернет и других видах операций. Код CVV можно найти на обратной стороне карты – это последние 3 цифры из семизначного числа рядом с местом для подписи, которые, как правило, визуально отделены от всего числа.

Схема мошенничества проста, потерпевшему с учетной записи знакомого приходит сообщение с просьбой оказать помощь в получении денежного перевода, пополнении баланса мобильного телефона (оператора сотовой связи РФ) и иной финансовой помощи. Ссылаясь на различные причины, связанные с неработоспособностью платежной карты либо отсутствием доступа к услугам интернет-банкинга, мошенники просят предоставить реквизиты платежной банковской карты. Достаточно было даже фотографии банковской карты с двух сторон. Пользователи, наивно полагая, что единственной защитой карт-счета является пин-код, беспечно предоставляли требуемую информацию злоумышленнику.

В текущем году возбуждено 16 уголовных дел по подобным фактам мошенничества. В настоящее время в органы внутренних дел области продолжают обращаться граждане, пострадавшие по этой схеме.

Также распространены случаи, когда пользователю, разместившему объявления о продаже имущества на торговых интернет-площадках, таких как «Куфар», «Онлайнер», поступают звонки от злоумышленника, который представляется лицом, заинтересованным в покупке продаваемого товара и, ссылаясь на то, что он находится в другом городе, предлагает внести предоплату на банковскую карту продавца. В ходе общения потерпевший сообщает реквизиты своей карты, паспортные данные злоумышленнику, а также код, поступивший в виде SMS-сообщения на его мобильный телефон. «Покупатель» уверяет, что это все необходимо для перевода денежных средств на карту потерпевшего, однако этих данных достаточно для того, чтобы осуществить хищение всех имеющихся денежных средств на карт-счете.

В результате проведенных оперативно-розыскных мероприятий сотрудниками отдела по раскрытию преступлений в сфере высоких технологий УВД установлено, что злоумышленники находятся на территории соседних государств, большинство из которых в Российской Федерации.

К информации, поступающей из сети Интернет, связанной с деньгами, следует относиться достаточно серьезно. Схемы мошенничества разнообразны: это и подобные просьбы о финансовой помощи, это и выигрыши в лотерее, всевозможные дополнительные заработки и т.д.

ОДНАКО ВСЕГДА СЛЕДУЕТ ПРИДЕРЖИВАТЬСЯ ГЛАВНЫХ ПРАВИЛ:

1. НЕ ЗАПИСЫВАЙТЕ ПИН-КОД НА КАРТЕ ИЛИ В ЛЕГКОДОСТУПНЫХ МЕСТАХ.

Почти 90% хищений денежных средств с пластиковых банковских карт – по причине халатного отношения к сохранению тайны пин-кода.

ТЕХНИЧЕСКИЙ ЛИКБЕЗ:

На магнитной полосе пин-код не записан в зашифрованном виде. Если у вас пропали деньги с карты и банк заявляет, что снятие было с использованием кода – сразу вспоминайте, кто мог видеть ваш пин-код, или, где вы могли его записать, кому-то сообщить.
Кстати, если операция проводилась с вводом пин-кода (банк это видит в отчётах) и в банкомате отсутствует система видеонаблюдения, у вас практически нет шансов вернуть ваши деньги. По правилам платёжных систем, такие операции нельзя опротестовать. Банк имеет полное право отказать в рассмотрении жалобы о краже денег, и будет совершенно прав.

ВЫВОД:

запоминайте пин-код или записывайте его так, чтобы никто не понял, что это он. Например, пин-коды можно хранить в качестве мобильных номеров вымышленных людей, зная, что пин – это первые четыре цифры номера Иванова И.И. и т.д.

2. НЕ ПЕРЕДАВАЙТЕ НИКОМУ РЕКВИЗИТЫ СВОЕЙ КАРТЫ.

Если конкретнее – номер карты, срок действия, имя и фамилия. По большому счёту, этого может быть достаточно для снятия денег с карты, даже без её физического присутствия. Не надо оставлять её на столе, т.к. даже за 10 секунд можно сфотографировать карту с двух сторон, чего будет достаточно, для снятия с них денежных средств.

3. ЕСЛИ РАСПЛАЧИВАЕТЕСЬ КАРТОЧКОЙ В МАГАЗИНЕ/РЕСТОРАНЕ/ГОСТИНИЦЕ, НЕ ДОПУСКАЙТЕ, ЧТОБЫ КАРТОЧКА ПРОПАДАЛА ИЗ ВИДУ.

Например, официант может сказать, что терминал находится там-то и ему нужно отойти, чтобы прокатать вашу карту. В этом случае вы имеете полное право требовать, чтобы он взял вас с собой. Никто ведь не знает, что он там собрался с ней делать. При помощи нехитрого технического устройства можно запросто сделать клон вашей карты и пытаться ей расплачиваться в торговых сетях. По своему опыту скажу, что на моей памяти, 80% всех мошеннических операций по картам, проходит при участии обслуживающего персонала торговой точки или сотрудника банка. Не нужно облегчать им задачу. Хотя, если уж на вашу карту «положат глаз», считайте, что пропажа денег - дело времени. Из этого плавно вытекают два следующих правила.

4. НИКТО НЕ ДОЛЖЕН ЗНАТЬ БАЛАНС ВАШЕЙ КАРТЫ.

Проверка баланса где-либо - это самая рискованная электронная операция по карте. Мошенники охотятся за балансами карт, а не за самими картами. Никогда не выбрасывайте балансовые чеки, не рассказывайте направо и налево, что у вас там куча денег и т.п.

5. ЗАВЕДИТЕ СЕБЕ ОТДЕЛЬНУЮ КАРТУ ДЛЯ БАНКОМАТОВ И КЛАДИТЕ НА НЕЁ ТОЛЬКО НУЖНУЮ СУММУ.

Не вздумайте копить деньги на карте, которую вы каждый день носите с собой. Откройте для этих целей любую карта уровня VisaElectron, MasterCardElectronic, CirrusMaestro. Эти карты открываются бесплатно либо за символическую плату. Обслуживание, как правило, тоже стоит копейки. При этом, желательно подобрать банк с бесплатным интернет - банкингом. Тогда будет удобно переводить деньги с накопительной карты на зарплатную.

6. БУДЬТЕ ПРЕДЕЛЬНО ОСТОРОЖНЫ С КРЕДИТНЫМИ (НА КОТОРЫХ ЕСТЬ КРЕДИТНЫЙ ЛИМИТ) КАРТАМИ.

Не используйте их в «сомнительных» местах. Проблема в том, что при потере денег с карты, вы теряете деньги банка. Как следствие – на вас будет висеть долг, да ещё под проценты.

7. ДЕРЖИТЕ В СВОЁМ МОБИЛЬНОМ ТЕЛЕФОНЕ НОМЕР СЕРВИСНОГО ЦЕНТРА БАНКА, ГДЕ ВЫДАЛИ ВАМ КАРТОЧКУ.

Этот номер записан на самой карте. И мы привыкли искать его именно там. Однако если карту похитили – начинаются беспорядочные метания в поисках нужного телефона.

ВЫВОД:

карту украли – сразу звоним в банк и блокируем.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ.

По мере развития сети Интернет, мы всё чаще начинаем использовать наши пластиковые карты для оплаты тех или иных товаров и услуг во всемирной паутине. Естественно, там где «ходят» какие-то деньги, всегда полно желающих эти самые деньги украсть. Причём, чем больше денег, тем больше желающих.
Чтобы сразу понять всю логику, вот вступительный ликбез: для того, чтобы снять деньги с вашей карты в Интернете, необходимо знать: номер карты, срок годности, имя, фамилию владельца, CVV код (эти 3 цифры можно увидеть на обратной стороне карты справа от полосы для подписи).
Немного о самом CVV коде. Этот код является неким аналогом пин-кода, который предназначен исключительно для Интернета. Берегите эти цифры, т.к. это онлайн-ключ к вашей карте.

ЕСЛИ НА САЙТЕ ВАС ПРОСЯТ ВВЕСТИ ПИН-КОД (НЕ CVV КОД) – 99% ЧТО ЭТО МОЖЕТ ОКАЗАТЬСЯ МОШЕННИЧЕСТВОМ.

Иногда на картах этот код не печатается. Это не значит, что его нет – он есть всегда. Просто позвоните в банк и вам его продиктуют.

ПРИЧЁМ, ЭТО ВСЕГДА 3 ЦИФРЫ, НЕ ПУТАЙТЕ С 4-МЯ ПОСЛЕДНИМИ ЦИФРАМИ НОМЕРА КАРТЫ, КОТОРЫЕ ЧАСТО ПЕЧАТАЮТ РЯДОМ.

К сведению: для Интернета лучше всего заводить карты уровня VISA Classic/MasterCardStandard. Более крутые карты в Интернете светить крайне не советую – их могут похитить. Вообще, идеальным вариантом будет открыть виртуальную карту, типа VISA Virtuon или её аналог. Такая карта 100% сработает на любых сайтах, да и на воровстве такой карты достаточно легко попасться.
По поводу карт дебитного класса (VISA Electron, MasterCardElectronic, CirrusMaestro) – такие карты принимают к оплате достаточно не охотно. Многие сайты просто отказываются принимать к оплате эти карты, т.к. изначально они создавались для использования в банкоматах, вследствие чего, платёжные системы не особенно следят за их безопасностью в сети. А принимать «опасные» карты к оплате – не выгодно.

СОВЕТЫ:

1. САМЫЙ ПЕРВЫЙ ПРИНЦИП – НЕ ОСТАВЛЯЙТЕ РЕКВИЗИТЫ СВОЕЙ КАРТЫ НА МАЛОЗНАКОМЫХ САЙТАХ (ДА И ВООБЩЕ, НИКУДА ИХ НЕ ПИШИТЕ, ЕСЛИ ВАС ОБ ЭТОМ НЕ ПРОСЯТ).

Наиболее яркие элементы, которые должны вызывать подозрение:

- когда сайт сделан не качественно
- весь сайт наполнен рекламой, всплывающими окнами;
- форма для реквизитов карточки находится на незащищённой странице (адрес защищённой страницы должен обязательно начинаться на https://).

2. ВЫБЕРИТЕ СЕБЕ НЕСКОЛЬКО САЙТОВ, КОТОРЫМИ ВЫ БУДЕТЕ ПОЛЬЗОВАТЬСЯ ВСЁ ВРЕМЯ.

Не нужно посещать множество сайтов, пытаясь найти ту или иную услугу/товар на пару рублей дешевле. Лучше не рисковать.

3. ХОРОШИЙ ВАРИАНТ, КОГДА ДЛЯ ВВОДА РЕКВИЗИТОВ КАРТЫ, ВАС ПЕРЕБРАСЫВАЮТ НА САЙТ БИЛЛИНГОВОЙ СИСТЕМЫ, А НЕ ПРОСЯТ ВБИВАТЬ РЕКВИЗИТЫ КАРТЫ ПРЯМО НА САЙТЕ.

Вы ведь не знаете, куда потом сайт отправляет ваши данные и насколько хорошо там отлажена система безопасности. По крайней мере, на сайте биллинговой системы вбивать реквизиты несколько безопасней.

4. ЗАВЕДИТЕ ДЛЯ ОНЛАЙН ОПЕРАЦИЙ ОТДЕЛЬНУЮ КАРТУ.

ПОМНИТЕ, ЧТО ЗА ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ПОХИЩЕННЫХ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК ПРЕДУСМОТРЕНА ОТВЕТСТВЕННОСТЬ, УСТАНОВЛЕННАЯ СТАТЬЕЙ 212 УГОЛОВНОГО КОДЕКСА РЕСПУБЛИКИ БЕЛАРУСЬ, КОТОРАЯ ПРЕДУСМАТРИВАЕТ НАКАЗАНИЕ ВПЛОТЬ ДО ЛИШЕНИЯ СВОБОДЫ НА СРОК ОТ 3 ДО 15 ЛЕТ.

ООПП Осиповичского РОВД