Профилактика преступлений в сфере высоких технологий на территории Брестской области

Уже ни для кого не секрет, что в настоящее время практически все трудоспособное население нашей страны так или иначе вовлечено в процессы, связанные с ресурсами сети Интернет. Естественно, все эти процессы оказывают очень существенное влияние на молодежную среду, проникновение которой в сеть Интернет и сферу высоких технологий оценено практически в 100%.

Все это происходят на фоне, в большинстве своем, минимальных познаний населения по индивидуальному обеспечению собственной информационной безопасности. Как следствие, в течение последних лет число выявленных преступлений, совершенных против информационной безопасности, ежегодно прирастает в разы. 90% таких преступлений совершаются людьми, не имеющими никакого специализированного образования в данной сфере. Киберпреступники — обыкновенные мошенники, жаждущие наживы, но выбранная «бизнес-модель» заставляет их быть очень изобретательными.

Преступность в сети Интернет приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег, практически полная безнаказанность, анонимность преступников, большое количество доверчивых людей – все это подпитывает этот своеобразный «бизнес».

В сети Интернее действуют те же законы, те же нравы, те же обычаи, что и в реальной жизни, в «оффлайне». Это же касается и противоправной деятельности, желание некоторых граждан обогатиться за чужой счет, утвердить собственное «я», получить власть над другими.

Состояние преступности в сфере высоких технологий

На протяжении последних лет число преступлений в сфере высоких технологий неуклонно продолжает расти. В 2019 году в области зарегистрировано **1095** таких преступлений (в 2018 - 728, +50,4%).

Справочно: рост высокотехнологичных преступлений отмечается по всей республике (+122,3%) и присущ каждому региону страны.

Анализ возбужденных уголовных дел по линии СВТ показал, что **рост преступлений в основном связан с обращениями граждан по фактам хищения денежных средств с использованием полученных обманным путем реквизитов банковских платежных карт** (далее - БПК).

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день в молодёжной среде мы вряд ли найдем кого-либо, кто не был бы зарегистрирован во «ВКонтакте», «Facebook», «Instagram», каких-либо тематических форумах или иных площадках для виртуального общения. В целом это норма, ведь человек живет в обществе

и стремится общаться. Однако некоторая неопытность, наивность и доверчивость порой приводит к негативным последствиям.

Основная проблема социальных сетей – это как раз доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека. Но с другой стороны, это открывает двери для злоумышленников.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив – он может создать ложное ощущение, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

Еще одна угроза, очень часто встречающаяся в настоящее время, – это взломом пользовательских учетных записей социальных ресурсов. Причин тому несколько и, прежде всего, – небрежное отношение пользователей к своим паролям.

Преступники прежде всего стремятся получить доступ к аккаунтам, которые защищены простыми паролями. Для этого они запускают программы, подбирающие пароли, и используют готовые словари и простые сочетания букв с цифрами. «Natashenka2019» — вариант, который программа проверит в числе первых, если почта заведена в 2019 году, а имя пользователя — «Наталья». Такие программы без труда определяют инвертированную раскладку и легко взломают к примеру пароль «vjqgfhjkm» (набранное в английской раскладке клавиатуры словосочетание «мойпароль»).

Составляя пароль, используйте комбинации букв, цифр, специальных символов, неочевидные ассоциации и сочетания различных элементов. Имя или номер телефона — не лучший выбор. Правильно оценивайте сложность пароля перед началом использования:

- **совсем слабый пароль:** общеизвестные аббревиатуры, названия, общеупотребительные фразы и слова (qwerty, admin, pass123, password, root; 4% пользователей используют пароли из первой десятки популярных, а три самых популярных пароля держат лидерство годами);
- п**лохой пароль, который кажется сложным:** дата вашего рождения или рождения кого-то из близких, номер какого-то из ваших документов, кличка вашего домашнего питомца, инверсия в раскладке простого слова, особенно, вашего имени, замена пары букв цифрами в применимом к Вам слове;

- **сложный пароль:** имеет не очевидную и не сводимую к одному слову основу для запоминания с обязательным использованием цифр, букв (со сменой регистра клавиатуры) и специальных символов.

Для создания достаточно сложного пароля всегда можно использовать онлайн-генератор паролей, которые зачастую предлагают пользователя несколько вариантов. Выбрав наиболее привлекательный, замените несколько символов на случайные, после чего используйте. Конечно же, запомнить такие пароли порой затруднительно, по этой причине их приходится записывать, однако делать это нужно соблюдая следующие рекомендации:

- записывайте пароль отдельно от логина или имени пользователя;
- записывайте его не полностью, а лишь частично или разделите пароль на части и поменяйте их местами;
- записывая пароль, зашифруйте его часть или добавьте заведомо для вас лишние символы.

Стоит также помнить, что использовать один пароль для доступа к разным аккаунтам не рекомендуется, так как каждый интернет-ресурс использует свои системы защиты и хранения паролей, которые не всегда могут быть реализованы на высоком уровне. Согласно статистике, около 14% пользователей используют один и тот же пароль для авторизации на всех аккаунтах и получив доступ к одному, злоумышленник непременно получит доступ и к другим.

Также внимательно отнеситесь к любым уведомлениям о неудачных попытках доступа к Вашему аккаунту и, в случае необходимости, смените пароль на более надежный.

Очень часто злоумышленники даже не пытаются взломать пароль, а просто стараются его узнать под тем или иным предлогом. Они массово рассылают письма и сообщения с призывом поучаствовать в беспроигрышной акции, проводимой крупной торговой сетью или финансовой организацией, при этом злоумышленники стараются оставить на раздумья как можно меньше времени, чтобы подтолкнуть пользователя на принятие решения немедленно, под влиянием эмоций. Зачастую, для участия в таких «акциях» требуется предоставить имя пользователя и/или пароль от какого-либо аккаунта или сведения о банковской платежной карте. Использование эффекта внезапности излюбленный прием злоумышленников: так, обнаруженное в электронном почтовом ящике письмо о якобы заблокированном аккаунте в социальной сети, очень часто толкает пользователей на переход по прикрепленной ссылке, которая в свою очередь ведет на поддельную страницу (очень похожую на настоящую), где для отмены блокировки необходимо вести свои данные. После ввода вся информация попадает в руки злоумышленников. Стоит запомнить, что пароль — это секрет, который должен принадлежать

только одному человеку, а если о нем знает кто-то еще, то это уже не секрет.

Таким образом, после совершения несанкционированного доступа к персональным аккаунтам, в течение первых суток зачастую развиваются следующие сценарии:

- злоумышленник рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты, при этом, хоть в большинстве своем школьники банковских карт не имеют, но желая помочь «другу» очень часто используют карты своих родственников и друзей. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы (практически во всех случаях хищения денежных средств со счетов мобильных телефонов потерпевшие еще сообщали преступнику персональные коды, приходящие в виде смс-сообщений на телефон).

Пример: возбуждено уголовное дело по факту хищения путем использования компьютерной техники (ст.212 УК) у жителя г.Жабинка 1998 г.р., денежных средств в размере 1000 рублей: 18 сентября неизвестный, направил ему сообщение в социальной сети «ВКонтакте» от имени курьера индивидуального предпринимателя с просьбой передать реквизиты банковской карточки и, получив их, похитил с карт-счета данную сумму.

Максимальное наказание за совершение хищений путем использования компьютерной техники – лишение свободы на срок от 5 до 12 лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью.

Анализ показывает, что **не более 20% людей, получивших такие сообщения, связываются с владельцем страницы, что в этой ситуации крайне важно.** Чтобы обезопасить себя от этого вида преступлений, не стоит сообщать никому реквизиты доступной банковской платежной карты или номер мобильного телефона и содержание смс-сообщений, поступающих для подтверждения совершения операции. **Ежедневно на территории области фиксируется несколько подобных случаев.**

- злоумышленник изучает содержание переписок потерпевшего и использует их содержание в качестве инструмента для вымогательства денежных средств. Таким образом, инструментом вымогательства становятся личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные. Обычно, перед тем как связаться с потерпевшим, преступник делает скриншот списка всех его друзей и близких. Избежать подобного

возможно лишь путем регулярной чистки своих диалогов и удаления из сети всей информации компрометирующего характера.

Например: неустановленное лицо со страницы в сети «ВКонтакте» осуществило переписку с жителем г.Бреста 1996 г.р. и под предлогом последующего вступления в интимные отношения получило от последнего интимные фото, после чего требовало от него перечислении 500 рублей за нераспространение фото в сети Интернет. Данное деяние квалифицируется как вымогательство (ст. 208 УК), наказание - штраф или исправительные работы на срок до 2 лет, или арест, или ограничение свободы на срок до 5 лет, или лишение свободы на тот же срок.

- злоумышленник начинает рассылать различного рода порочащую информацию от имени владельца страницы иным пользователям, ссылки на поддельные ресурсы банковских учреждений, а также вредоносное программное обеспечение, что также может привести к серьезным последствиям.

В случае обнаружения «взлома» аккаунта, прежде всего, следует попытаться восстановить доступ наиболее привычным способом, путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, кроме этого следует оповестить друзей и знакомых об инциденте, используя при этом иные социальные сети и мессенджеры. Кроме этого, чтобы в какой-то мере обезопасить себя от взлома, специалисты по безопасности рекомендуют «привязать» страницу социальной сети именно к номеру мобильного телефона, а не к адресу электронной почты, при этом вход на Вашу страницу с неизвестного компьютера или мобильного телефона будет не возможен без знания кода, который будет выслан на указанный при регистрации страницы номер.

Как не стать жертвой преступлений против информационной безопасности

Основным источником опасности для пользователей компьютеров и иных цифровых устройств были и остаются вредоносные программы, которые с развитием сетевых технологий получили новые возможности распространения и дополнительный, зачастую малозаметный пользователю функционал:

- вредоносное программное обеспечение может зашифровать данные на компьютере за расшифровку которых потребуют «выкуп».

- компьютер может начать работать медленно и со сбоями, потому что без вашего ведома его используют для атак на другие сайты или майнинга криптовалюты.

Справочно: майнинг, также добыча – деятельность по созданию новых структур (новых блоков в блокчейне) для обеспечения функционирования криптовалютных платформ.

- у вас могут похитить личные данные, пароли от почтовых аккаунтов, страниц в социальных сетях.

- злоумышленники получат доступ к вашим платежным системам и личным кабинетам в банках. С ваших счетов будут сняты деньги, с помощью ваших карт расплатятся за чужие покупки в Интернете.

Так, в мае т.г. неустановленное лицо через систему интернет-банкинга одного из белорусских банков, установленную на компьютере предприятия ввело в компьютерную систему ложную информацию об использовании расчетного счета, реквизитов фирмы, ключа и пароля его держателем, получило несанкционированный доступ к расчетному счету предприятия, при этом похитило в 7 приемов денежные средства в размере 35 тысяч рублей.

Чтобы не стать жертвой преступлений против информационной безопасности, следует неукоснительно следовать **правилам информационной безопасности:**

• не устанавливать программное обеспечение из неизвестных источников;

• не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы;

• использовать наиболее современную версию антивирусного программного обеспечения;

• использовать безопасные (сложные) пароли, а также механизмы дополнительной аутентификации;

• хранить пароли в тайне даже от близких;

• не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.) ни под какими благовидными предлогами.

Как не стать жертвой хищений с использованием компьютерной техники

С развитием интернет-технологий в финансовом секторе данный вид угроз приобретает все большую актуальность, а для совершения подобного рода преступлений преступники используют различные способы, начиная от физического завладения картой и использования бесконтактного способа оплаты в магазинах и заканчивая использованием реквизитов наших карт для совершения операций в сети Интернет.

Существуют специальные устройства, с помощью которых преступники получают информацию о данных чужих банковских карточек. Они называются **«скимеры»**. Их, как правило, устанавливают в район щели картоприемника банкомата и маскируют. При вставлении пользователем банковской карточки в банкомат, ее данные считываются устройством. Для того, чтобы кроме данных с магнитной полосы банковской карточки преступник получал также и данные pin-кода, чаще

используется встроенная видеокамера. Поэтому, подойдя к банкомату, необходимо убедиться, что на нем нет никаких «лишних» устройств.

Кроме этого, в настоящее время очень широкое распространение получили такие способы как:

- **звонок от «представителя» банка** с просьбой срочно предоставить необходимую информацию. Преступники сообщают, что необходимо осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Только за последние две недели в правоохранительных органах области зарегистрировано более 70 подобных фактов. Следует отметить, что преступники используют современные возможности сети Интернет и в частности возможность «подмены номера», как следствие у потерпевшего на экране мобильного телефона может отображаться совершенно любой абонентский номер телефона, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным.

Следует обращать внимание на то, что сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен.

Если Вам поступил такой звонок, то:

- ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме. В случае если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и Банк это заметит, то его сотрудники сперва инициативно заблокируют Вашу банковскую платежную карту, после чего сообщат Вам причину принятого решения (ничего не уточняя) и пригласят в свое учреждения с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;
- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на

экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;

- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения. Даже в этом случае не сообщайте никакой информации собеседнику;
- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего специалист сообщит Вам, что никаких несанкционированных операций зафиксировано не было, а сотрудник Банка Вам не звонил.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта. Помните, что если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства.

- **звонок по объявлению** с предложением приобрести продаваемый Вами товар. При этом преступник предлагает перевести предоплату на Вашу карту, реквизиты которой просит ему предоставить. Важно помнить, что для совершения перевода нужны данные лишь лицевой стороны, а если поступают просьбы предоставить еще и код, нанесенный с оборотной стороны или содержание смс-сообщений, которые как раз начинают поступать из банка – то это наверняка злоумышленник, пытающийся похитить деньги. Наиболее оптимальным способом обезопасить себя будет открытие дополнительной банковской карты, которая будет предназначена лишь для совершения оплат в сети Интернет и на которой не будут хранится денежные средства. В настоящее время многие банки предоставляют возможность оформления даже виртуальных карт совершенно бесплатно.

Пример: в ноябре 2019 года возбуждено уголовное дело по заявлениям 4 жителей Пинска, о том, что неизвестный с 28 по 30 октября, в ходе телефонного разговора, представившись работником банковской организации, находясь в неустановленном месте, завладел реквизитами банковских карточек и похитил с карт-счетов 225, 138, 1800 и 220 рублей соответственно.

Чтобы не стать жертвой подобных преступлений:

1. Обязательно подпишите карточку и храните в тайне ПИН-код к ней. Для обеспечения безопасности ПИН-кода запомните его или храните отдельно от карточки в неявном виде, но ни в коем случае не записывайте на самой карточке. Помните, что независимо от обстоятельств никто не вправе требовать от Вас значение ПИН-кода: ни представители правоохранительных органов, ни кассиры торговых точек, ни представители банка.
2. Храните карточку в безопасном месте, исключая доступ к ней третьих лиц. Не оставляйте карточку на виду, чтобы предотвратить несанкционированное копирование реквизитов карточки *(номер карточки, срок её действия, проверочный код CVV2/CVC2).*
3. Помните, что банки не рассылают писем, SMS-сообщений, электронных сообщений с просьбой подтвердить реквизиты карточки, ПИН-код или иную личную информацию. Если вы получили по телефону либо e-mail сообщение о необходимости предоставления реквизитов карточки, ввода их на каком-либо сайте либо совершения какой-либо операции в банкомате – ни в коем случае не доверяйте такой информации. Если в сообщении содержится информация о том, что Ваша карточка была заблокирована, уточните факт блокировки карточки в круглосуточной Службе сервиса клиентов.
4. Установите лимиты расходования средств и подключите услуги оповещения о транзакциях.
5. При снятии денежных средств в банкомате обращайте внимание на людей, стоящих за вами в очереди. В случае необходимости попросите их отойти на расстояние, при котором они не могут увидеть вводимый ПИН-код. Набирайте ПИН-код быстро, заученными движениями и желательно несколькими пальцами. При вводе ПИН-кода на клавиатуре прикрывайте клавиатуру рукой, кошельком или сумочкой.
6. При проведении операции в организациях торговли и сервиса не выпускайте карточку из вида. При необходимости проследуйте к месту установки терминала для проведения оплаты.
7. Обращайте особое внимание на действия кассира. Если он пытается провести карточку через терминал более одного раза, уточните причину повторного использования карточки (такой причиной может быть, как технический сбой, так и попытка несанкционированного доступа к Вашим данным).

Для совершения операций за пределами Республики Беларусь, либо с использованием сети Интернет рекомендуется:

1. Открыть отдельный счет и пополнять его по мере необходимости (например, с помощью услуги перевода средств между карточками в системе «Интернет-банкинг»).

2. По возвращении из поездки желательно перевести денежные средства на другой счет.

3. При выборе карточки предпочтение следует отдать карточке с чипом (стандарт EMV), т.к. она имеет более высокий уровень безопасности и лучше защищена от подделки.

4. Не рекомендуется использовать за границей сберегательные карточки.

5. Установите лимиты расходования средств и подключите услуги оповещения о транзакциях.

6. При обнаружении пропажи карточки, подозрении на совершение мошеннических операций либо, в случае изъятия карточки банкоматом или кассиром в торговой точке или пункте выдачи наличных, следует как можно быстрее заблокировать карточку.

7. При выборе терминала отдавайте предпочтение тому устройству, которое расположено в хорошо освещенном людном месте.

Соблюдение этих несложных мер предосторожности позволит уберечь ваши денежные средства от преступных посягательств.