Сегодня мы живем и работаем в мире глобальных возможностей взаимодействия. Посредством Интернет можно вести легкомысленную беседу или совершать многомиллионные денежные операции и сделки с людьми с другой стороны планеты быстро и недорого. Стремительное увеличение количества персональных компьютеров, свободный доступ к Интернету и быстро развивающийся рынок новых коммуникационных устройств изменили и способы проведения досуга, и методы ведения бизнеса.

Новые возможности, появившиеся в результате развития информационных технологий, а также широкое их использование в повседневной жизни и создание на их основе глобальных компьютерных сетей, как неотъемлемой части современной деятельности, создают предпосылки, облегчающие совершение преступных деяний. Распространение компьютерных вирусов и детской порнографии, мошенничества с пластиковыми платежными карточками, хищение денежных средств с банковских счетов – это далеко не полный перечень подобных преступлений, которые получили распространенное название «киберпреступность», также наблюдается опасная тенденция сращивания «киберпреступности» с транснациональной и организованной преступностью. При этом лицо, совершившее преступление, часто остается анонимным, может находиться на другой стороне земного шара, и при этом следы преступления в виде все той же компьютерной информации легко уничтожаемы.

Сегодня, многие из нас, пользуются Интернетом – **практически у всех есть страница в социальных сетях, электронные почтовые ящики.** В Интернете, на компьютерах мы храним наши персональные данные, однако, мало кто из нас задумывается, что электронные средства хранения более уязвимы, чем бумажные. Размещаемые посредством электронных средств хранения данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Из года в год количество преступлений, совершенных с использованием компьютерных технологий, неизменно растет.

Значительное увеличение указанных преступлений связано с ростом несанкционированных доступов к личным страницам граждан в социальной сети, вследствие чего злоумышленники, используя методы социальной инженерии, получают у знакомых владельцев страниц реквизиты банковских платежных карт, с которых в последующем совершаются хищения денежных средств.

Так, злоумышленник под аккаунтом ничего не подозревающего пользователя сети, с целью получения корыстной выгоды рассылает сообщения его знакомым и друзьям.

Например, при взломе страницы в социальной сети гражданина А. злоумышленник разослал сообщения его друзьям с просьбой перевести

Phoca PDF

денежные средства на абонентские номера компании связи, зарегистрированной в Российской Федерации. При этом в сообщениях от его имени он написал, что находится в трудной жизненной ситуации и ему в срочном порядке требуются деньги. Друзья пользователя сети, предполагая, что оказывают помощь гражданину А., перевели денежные средства на указанные злоумышленником номера абонентов мобильной сети.

При этом сам гражданин А. находился по месту жительства и никто из его товарищей не догадался позвонить ему и спросить что же с ним случилось.

В другом случае злоумышленник, осуществив несанкционированный доступ к странице в социальной сети гражданки Б. и воспользовавшись ее аккаунтом, от ее имени переслал сообщения зарегистрированным в сети ее друзьям с просьбой указать реквизиты своих банковских карт. Злоумышленник, при пересылке сообщений пользовался данными, хранящимися на странице в социальной сети, а именно использовал способ переписки, словесные обороты, жизненные события, отраженные в предыдущих сообщениях гражданки Б. и ее друзей.

Чтобы избежать подобного рода хищений, необходимо в первую очередь соблюдать правило – не указывать свои персональные данные, реквизиты банковских карточек, логины, пароли и иную конфиденциальную информацию в глобальной сети Интернет.

С целью недопущения несанкционированного доступа к компьютерной информации, необходимо защитить установленный пароль.

Следует помнить:
• нельзя делиться своим паролем;
• для создания пароля нужно использовать строчные и прописные буквы вперемешку с цифрами, либо позволить компьютеру самому сгенерировать пароль;
• предпочтительно использовать длинные пароли, так как они более безопасны;
• не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;
• пароль не должен отображаться на экране компьютера при его вводе;
• пароли должны отсутствовать в распечатках; нельзя записывать пароли на столе, стене ином видном месте, его нужно держать в памяти.

Помимо этого:

1. **Не записывайте пин-код на карте или в легкодоступных местах.** Почти 90% хищений денежных средств с пластиковых банковских карт – по

Phoca PDF

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 отчетах) 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 счету, этого может быть достаточно для снятия денег с карты, даже без ее 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**

Phoca PDF

только нужную сумму. Не вздумайте копить деньги на карте, которую вы каждый день носите с собой. Откройте для этих целей любую карта уровня Visa Electron, Master Card Electronic, Cirrus Maestro. 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 своем 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.

По материалам Романа РОМАНЕНКО.

Phoca PDF