МАТЕРИАЛЫ
для проведения профилактической работы
с населением по предупреждению
преступлений в сфере высоких технологий

В текущем году на территории области наблюдается более чем трехкратный рост количества зарегистрированных киберпреступлений. За 11 месяцев учтено 859 таких преступлений, 65% из которых – хищения путем использования компьютерной техники. Общая сумма ущерба по преступлениям (без учета покушений) в области превысила 315 тысяч рублей, в республике – 4,7 миллиона рублей.

В том числе в ноябре в области учтено 96 фактов хищений с карт-счетов граждан, 77 из которых были совершены в сети Интернет, в результате чего держатели карт потеряли около 70 тысяч рублей. Средняя сумма хищения в последний месяц составила около 725 рублей, максимальная – 6 900 рублей.

Среди актуальных на сегодняшний день видов преступлений, совершаемых в отношении физических лиц, необходимо выделить:

– завладение денежными средствами с карт-счета с использованием соцсетей;
– хищение с карт-счета с использованием вишинга по телефону;
– завладение денежными средствами с карт-счета с использованием фишинга;
– несанкционированный доступ к учетной записи в соцсети, электронной почте.

В отношении предприятий и организаций совершаются следующие противоправные деяния:

– блокирование компьютерной информации путем ее шифрования с целью предъявления требований о денежной компенсации за разблокировку;
– заражение ПЭВМ вредоносным программным обеспечением (банковскими троянами) с целью дальнейшего хищения денежных средств предприятия через систему дистанционного банковского обслуживания.

Рассмотрим их подробнее.

Зачастую имеет место с ситуация, когда со взломанной либо подложной учетной записи **в соцсети** осуществляется рассылка сообщений с целью перевода денежных средств либо передачи реквизитов банковской платежной карточки либо учетной записи в системе Интернет-банк. Например:

– «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом переведешь мне, когда мою карту разблокируют. В долгу не останусь!»;

– «Какого банка у тебя карточка? Мне нужна VISA или MasterCard для оплаты в интернете. Можешь дать реквизиты или сфотографировать? Там еще на обратной стороне три цифры есть. Тебе на телефон должен придти код, напиши сюда. Нет, не беспокойся, я деньги верну с комиссией.»;
– «Можешь дать логин и пароль от интернет-банкинга. В моем выдает какую-то ошибку, хочу проверить, есть ли в твоем такой баг. Платежей делать не буду, мы же друзья!»

Трендом ноября текущего года является **вишинг** — форма мошенничества, основанная на социальной инженерии. Злоумышленники, используя телефон и играя определенную роль (например, сотрудника банка), под разными предлогами выманивают персональные данные (например, реквизиты платежных карт), чтобы заполучить денежные средства клиентов банков.

Предлогом для передачи данных могут быть:
– осуществление по карте мошеннической операции и необходимость срочной ее отмены;
– оформление через интернет-банкинг онлайн-кредита и принятие срочных мер по его отклонению и т.д.

При этом в зависимости от ситуации злоумышленники пытаются завладеть следующей информацией:
– идентификационный номер и иные паспортные данные;
– номер карты, срок действия, имя владельца, CVV/CVC-код;
– коды подтверждения, приходящие на Ваш номер телефона;
– реквизиты доступа к системе Интернет-банк (логин, пароль, сеансовый ключ).

Еще одним способом завладения реквизитами является **фишинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения рассылок электронных сообщений, в которых содержится ссылка на сайт, внешне неотличимый от настоящего.

После того как пользователь попадает на поддельную страницу, мошенники пытаются побудить пользователя ввести на поддельной странице свои логин и пароль доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Также в результате проведенного анализа обозначены возможные причины заражения корпоративных ПЭВМ:
– ошибки в настройке системы безопасности локальной сети;
– использование устаревшего либо контрафактного программного обеспечения, не поддерживаемого производителями;

– использование программного обеспечения, полученного из сомнительных источников;
– отсутствие обновляемого антивирусного программного обеспечения;
– посещение пользователями подозрительных Интернет-ресурсов;
– просмотр пользователями входящих электронных писем от незнакомых собеседников и открытие прилагаемых файлов. Зачастую злоумышленники рассылают письма с приложением документов, архивов, исполняемых файлов, под которые маскируется вредоносное программное обеспечение.

Во избежание различного рода киберинцидентов на уровне пользователя можно дать следующие рекомендации:
– использовать сложные пароли и периодически их менять;
– не сохранять пароли в браузерах, не хранить их на бумажных носителях в доступных местах;
– использовать антивирусное программное обеспечение;
– устанавливать приложения только из проверенных источников;
– не переходить по подозрительным ссылкам, не открывать подозрительные письма и вложения к ним;
– не использовать для переписки e-mail, к которому привязаны устройства, учетные записи, Интернет-банкинг;
– обмениваться сообщениями в мессенджерах только полностью удостоверившись в личности собеседника.

Держателям карточек необходимо:
– внимательно ознакомиться с правилами пользования банковскими платежными карточками Вашего банка;
– не передавать карту и ее реквизиты третьим лицам;
– использовать отдельную карту для Интернет-покупок и не хранить на ней деньги;
– подключить услуги 3D-Secure, SMS-информирование, установить необходимые лимиты;
– осуществлять оплату в сети Интернет на проверенных ресурсах, работающих по безопасному протоколу https.

В любой ситуации необходимо проявлять бдительность и помнить, что абсолютное большинство киберпреступлений становятся возможными ввиду неосмотрительности со стороны самого слабого звена информационной системы – человека.

ОРПСВТ КМ УВД
Гродненского облисполкома