Конспект на тему: «Предупреждение мошенничеств, в т.ч. совершаемых с использованием компьютерной техники»

Сегодня в повседневной жизни используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Первый из видов – это телефонное мошенничество.

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом.

Чаще всего в сети телефонных мошенников попадаются пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

К основным схемам телефонного мошенничества относятся:

SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счет.

Как это организовано: к примеру, абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 100 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Вторая схема – телефонный номер-грабитель

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

Например, вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со

связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь - и оказывается, что с Вашего счёта списаны крупные суммы.

На самом деле происходит следующее: существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный.

Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

Встречается и такой вид, как **телефонные вирусы**.

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: *«Вам пришло MMS-сообщение. Для получения пройдите по ссылке...».* При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: *«Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0».* При отправке подтверждения, со счета абонента списываются денежные средства.

Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.

Не следует звонить по номеру, с которого отправлен SMS - вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Достаточно распространены в последнее время случаи мошенничества с использованием банковских карт.

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Рекомендуем всем владельцам пластиковых карт следовать правилам безопасности:

никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами. Нельзя хранить ПИН-код рядом с картой и тем более

записывать ПИН-код на неё - в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

Не позволяйте никому использовать Вашу пластиковую карту - это всё равно, что отдать свой кошелёк, не пересчитывая сумму в нём.

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне - это Ваша ответственность и обязанность.

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка.

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком - он обязан предоставить консультационные услуги по работе с картой.

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Общие рекомендации по обеспечению безопасной работы в интернете:

1. Антивирусные программы

Установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы.

Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. Обновления

Отслеживайте появление новых версий операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.

Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления.

Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. Настройте свой компьютер против вредоносных программ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. Проверяйте новые файлы

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять.

5. Будьте бдительны и осторожны

По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

Помните, если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия - незамедлительно обратитесь в ближайший отдел милиции.

Ответственность за мошенничество предусмотрена ст. 209 Уголовного кодекса Республики Беларусь.

1.Завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием (мошенничество) -

наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Мошенничество, совершенное повторно либо группой лиц, -

наказывается исправительными работами на срок до двух лет, или ограничением свободы на срок до четырех лет, или лишением свободы на тот же срок.

3. Мошенничество, совершенное в крупном размере, -

наказывается лишением свободы на срок от двух до семи лет с конфискацией имущества или без конфискации.

4. Мошенничество, совершенное организованной группой либо в особо крупном размере, -

наказывается лишением свободы на срок от трех до десяти лет с конфискацией имущества.

УОПП МОБ УВД гродненского облисполкома