Министерство внутренних дел Республики Беларусь

Предупреждение хищений с использованием компьютерной техники.

С учетом быстрого развития информационных технологий в Республике Беларусь за очень короткий промежуток времени количество пользователей сети Интернет нашей страны превысило пять миллионов человек. По плотности проникновения широкополосного доступа на 100 человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире.

Проникновение информационных технологий во все сферы жизнедеятельности наших граждан наряду со слабым их пониманием определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

2021

В настоящее время каждый знает, что такое интернет, с развитием всемирной сети практически каждый ежедневно пользуется ресурсами интернета. Известно, что глобальная сеть, прежде всего, является неиссякаемым источником информации и полем для виртуального общения.

Однако далеко не все знают, какой ущерб может быть нанесен персональному компьютеру пользователя или самому пользователю.

Безопасность в сети интернет является довольно актуальной проблемой, которую полностью разрешить практически невозможно, так как вредоносные программы и сайты все время совершенствуются.

Как правило, жертвами злоумышленников, так называемых киберпреступников, становятся рядовые пользователи, не имеющие глубоких познаний в информационных технологиях.

Основными тенденциями киберпреступлений в 2021 являются:

- Социальная инженерия: хищение реквизитов банковских платежных карт белорусских граждан с использование «фишинговых» интернет-ресурсов и в результате взлома учетных записей пользователей социальных сетей, а также выманивание реквизитов банковских карт в результате телефонных звонков от имени сотрудников банковских учреждений, правоохранительных органов и т.д.

- Вирусы-шифровальщики: вирусные атаки на серверы предприятий с последующим шифрованием хранящихся на серверах файлов и требованием выкупа за расшифровку).

- Банковские вирусы-трояны: вирусная атака на серверы и ПЭВМ предприятия с целью установления несанкционированного удаленного управления «Клиент-банком» с последующим доступом и управлением банковскими счетами предприятия и перевода денежных средств на подставные кампании.

Как правило, жертвами злоумышленников, так называемых киберпреступников, становятся рядовые пользователи, не имеющие глубоких познаний в информационных технологиях.

Информация, представляющая интерес для киберпреступников:

- сведения о финансовых операциях;

- сведения о банковских счетах граждан;

- идентификационные данные платежных банковских карт и электронных платежных систем;

- иная информация конфиденциального характера и персональные данные.

На фоне интенсивного инновационного развития в Беларуси, культура пользования возможностями электронных помощников у граждан нашей республики по-прежнему остается на низком уровне. Большая часть белорусских пользователей легкомысленно относятся к угрозам, с которыми могут столкнуться в сети Интренет, а также

ответственности, которая их ждет за нарушение закона в сфере информационной безопасности.

ИТАК, БЕЗОПАСНОСТЬ.

Существует две угрозы для пользователей сети, это технические угрозы и социальная инженерия

К техническим угрозам относятся вредоносное программное обеспечения или вирусы такие как черви, трояны, руткиты и иные разновидности. Они представлены разнообразными видами и модификациями, которые постоянно развиваются.

Вирусы предназначены для нарушения работы компьютера, скрытого сбора данных о пользователе компьютера, таких как личных данных, паролей, документов, фотографий, размещенных в компьютере, для последующего вымогательства либо для передачи третьим лицам, так же для удалённого управления компьютером.

Не редко зараженные устройства будь это ПЭВМ, планшет или смартфон становятся частью «бот сети» позволяющей злоумышленнику выполнять некие противоправные действия с использованием ресурсов заражённого компьютера который входит в сеть таких же зараженных компьютеров.

И так что же может делать вирус на Вашем ПК:

- собирать информацию о привычках пользования интернетом и наиболее часто посещаемых сайтах.
- запоминать нажатия клавиш на клавиатуре, записывать скриншоты экрана и в дальнейшем отправлять информацию создателю вируса;
- несанкционированно и удалённо управлять компьютером;
- устанавливать на компьютер дополнительные программы;
- изменять параметры операционной системы;
- перенаправлять тебя в браузерах на сайты, которые заражены другими вирусами.

КАК ЖЕ МОЖНО ЗАРАЗИТЬ ВИРУСОМ УСТРОЙСТВО:

- через нелицензионное (пиратское) программное обеспечение, при установке его на ПК, т.к. в нем уже встроено вредоносное программное обеспечение.
- посещении сомнительных Интернет-ресурсов и скачивание с них определенного контента.
- при открытии вложенных документов в электронные письма, а также при переходе по ссылке для скачивания чего либо, которая указана в электронном письме.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

– метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека.

Основной целью социальных инженеров, как и других хакеров и взломщиков, является получение доступа к защищенным системам с целью кражи информации, паролей, данных о кредитных картах и т. п.

Основным отличием от стандартной кибератаки является то, что в данном случае в роли объекта атаки выбирается не машина, а пользователь. Именно поэтому все методы и техники социальных инженеров основываются на использовании слабостей человеческого фактора, что считается крайне разрушительным, так как злоумышленник получает информацию, например, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего.

ВИДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ:

самый распространенный и, наверное, самый актуальный вид, это ФИШИНГ. Самое интересное, что большинство про это знают, но все равно попадаются «на удочку» злоумышленников.

Цель фишинга – это получение доступа к конфиденциальным данным, таким как адрес, телефон, номера кредитных карт, логины и пароли, путем использования поддельных веб-страниц.

Часто фишинговая атака происходит следующим образом: на электронную почту приходит письмо с просьбой войти в систему Интернет-банкинга от имени якобы сотрудника банка. Письмо содержит ссылку на ложный сайт, который трудно отличить от настоящего. Пользователь вводит личные данные на поддельном сайте, а злоумышленник перехватывает их. Завладев персональными данными, он может, например, получить кредит на имя пользователя, вывести деньги с его счета и расплатиться его кредитными картами, снять деньги с его счетов.

Так же сообщение может прийти и в менеджере (вотсап, вайбер и др.). Мошенники изменяют один символ в названии сайта либо телефона банка, либо иной организации.

Еще один пример, всплывающее окно о каком-нибудь большом выигрыше денежном либо ином (айфон, автомобиль и т.д.) при нажатии на данное окно пользователь переходит по ссылке где ему предлагается ввести свои личные данные, данные для входа в учетную запись социальной сети либо данные банковской платежной карты, которые в последствии достанутся злоумышленнику.

Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

Статья 212. Хищение имущества путем модификации компьютерной информации

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Хищение имущества путем модификации компьютерной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

В последнее время все чаще фиксируются факты хищений с использованием реквизитов карт при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

Пример такого преступления: У Серегина Д.А. появилась необходимость в оплате коммунальных услуг посредством интернета, с использованием реквизитов его платежной банковской карты. Так как сам он ранее платежей посредством сети интернет не совершал, то попросил помочь ему в этом своего коллегу по работе Рыжикова В.В. Серегин Д.А. написал реквизиты своей платежной карты на лист и передал его Рыжикову В.В. Рыжиков В.В. посредством мобильного телефона Серегина Д.А. осуществил все необходимые платежи, после чего Серегин Д.А. ушел домой. Вечером этого же дня Рыжикову понадобилось перевести на счет в интернет игре денежные средства, и для этого он решил воспользоваться реквизитами платежной карты

Серегина, которые у него остались записанными на листе. Рыжиков В.В. ввел реквизиты платежной карты в форму для совершения перевода денежных средств и без каких либо проблем перевел денежные средства в размере 100 рублей. Таким образом Рыжиков В.В. совершил преступление, предусмотренное ст. 212 УК Республики Беларусь.

Также одной из разновидностей хищений денежных средств с использованием компьютерной техники, который появился относительно недавно и все чаще встречается на территории Республики Беларусь, это так называемый «вишинг». При совершении такого преступления злоумышленник обманным путем завладевает реквизитами платежных карт граждан и совершает с их помощью хищения денежных средств.

Пример такого преступления: Ивановой Р.А. посредством мобильного телефона позвонил не известный ей молодой человек, который представился сотрудником безопасности банка. Далее он пояснил, что с ее платежной банковской карты осуществляются попытки совершения несанкционированных платежей, которые банк отклоняет. Ей следует сообщить реквизиты ее платежной карты, что бы сотрудники банка ее заблокировали, и в последствии получить новую платежную карту. Когда Иванова Р.А. сообщила реквизиты своей платежной карты ей данный молодой человек пояснил, что сейчас ей на ее мобильный номер телефона придет СМС-сообщение, которое ей отправят сотрудники банка. Код в данном сообщении она должна сообщить для блокировки карты. После передачи кода, который находился в СМС-сообщении, с счета платежной карты Ивановой Р.А. были переведены все ее денежные средства.

Выводы и рекомендации

В 2020-2021 годах на территории Республики Беларусь наблюдается отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Сначала преступник получает несанкционированный доступ к средству связи с потенциальным потерпевшим, обычно это учетные записи в социальных сетях, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями. Обычно это становится возможным ввиду небрежного отношение владельца сайта к обеспечению сохранности конфиденциальной

информации (логинов, паролей) о пользователях либо беспечности самих пользователей. При этом такая беспечность со стороны пользователей может проявляться в:

- попадании «на удочку» лиц, создавших «фишинговый» (имитирующий настоящий) сайт;

- вводе логинов и паролей от своих учетных записей в соцсети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;

- использовании идентичных реквизитов для авторизации на различных ресурсах;

- использовании слишком легких паролей;

- отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

- «Я нахожусь за рубежом, я потерял свой кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах или других) 5 000 рублей. Все верну когда вернусь.»;

- «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а мне нужно с интернет кошелька вывести свои денежные средства. Можно я дам реквизиты твоей карты, на нее придут деньги, потом отдашь мне.»;

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение имущества путем модификации компьютерной информации». При этом надеяться на

то, что преступник в данной ситуации оставит на Вашем карт-счете хоть какую-то сумму, к сожалению, не приходится.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети Интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

- для выхода в сеть Интернет используйте устройства, на которых установлено антивирусное программное обеспечение;

- используйте операционную систему с установленными обновлениями безопасности;

- при использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно Вы зашли на поддельную его копию;

- не используйте одинаковые логины и пароли на различных сайтах;

- не используйте слишком легкие пароли, либо те, о которых можно легко догадаться;

- по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

- остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;

- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи;

- если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

- при осуществлении Интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ.

УПК КМ ГУВД Мингорисполкома