Методический материал для кураторского часа по повышению цифровой грамотности

В Республике Беларусь за последнее время значительно увеличилось количество преступлений в сфере высоких технологий или с их применением (согласно данных МВД Республики Беларусь их число возросло в разы по сравнению с прошлыми годами), в том числе расширяется перечень совершаемых посредством гаджетов наказуемых деяний.

На сегодняшний день существует множество способов совершения преступлений в сфере информационно-коммуникационных технологий.

Так, например, злоумышленники в целях получения платежных реквизитов зачастую представляются банковскими работниками, сотрудниками правоохранительных органов, знакомыми, и вводят в заблуждение жертв, ими разработан целый арсенал предлогов. Также имеют место случаи, когда злоумышленники используют фишинговые сайты - это многостраничные лжеплатформы, которые до мельчайших деталей копируют привычные интерфейсы популярных сайтов, или сайтов финансовых учреждений, но единственное, что кроется в названии ресурса то, что оно лишь от части повторяет оригинальное.

Также значительно увеличилось и число хищений денежных средств с банковских счетов, балансов абонентских номеров и т.д., где потерпевшие сами предоставляют необходимые для удаленного доступа конфиденциальные сведения злоумышленникам, которые используют телефонную коммуникацию и играют определенную роль (знакомого, сотрудника банка, покупателя и т.д.). Новые жертвы так называемого вишинга появляются ежедневно (вишинг - это один из методов мошенничества с использованием социальной инженерии с помощью телефонного звонка. На телефон поступает звонок от сотрудника банка и оператор предупреждает, если прямо сейчас не будет предоставлена полная информация банковской карты по телефону, то карту заблокируют. Доверчивый пользователь, слыша, подобную «угрозу» сразу же впадает в панику и может выдать все персональные данные, вплоть до проверочного кода из смс-сообщения. Также при вишинге может быть предложена выгодная покупка с огромной скидкой или озвучена информация о выигрыше в какой-либо акции. Не нужно сразу же радоваться столь удачной покупке или выгодной акции, всегда стоит лишний раз перепроверить информацию, обратившись к официальным ресурсам).

Гомельским городским отделом Следственного комитета Республики Беларусь проводится активная работа по профилактике совершения преступлений в сфере информационных технологий, а

именно: за период с 2020 по 2023 годы неоднократно доводилась информация до граждан посредством теле- и радиовещания, посредством печати предупреждающей информации в печатных средствах массовой информации и т.д.

Необходимо отметить, что наиболее подверженными становятся авторы объявлений о продаже товаров или сдаче в наем жилья. Едва услышав от якобы заинтересованных клиентов обещание перевести задаток, жертвы утрачивают бдительность и в предвкушении прибыли сообщают незнакомцам не только номер карты, но также и пароли, логины и даже коды из СМС-сообщений, необходимые для авторизации в какой-либо системе. После этого злоумышленники в считанные минуты добираются до чужих счетов и снимают все денежные средства.

Однако несмотря на многочисленные предупреждения, а также информацию, которая содержится в новостных лентах медиаресурсов, средствах массовой информации, потерпевшие обнародуют платежные реквизиты под натиском злоумышленников с использованием социальной инженерии.

Злоумышленники неустанно проводят обновление устаревших криминальных схем и поначалу обкатывают «новинки» за рубежом, а после переключатся на еще не обжегшихся жителей других государств.

СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИМУЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Надежные пароли:

необходимо:

- доверять только проверенным менеджерам паролей;
- создавать персональные (уникальные) пароли к разным сервисам;
- использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы;

не рекомендуется:

- использовать повторения символов;
- хранить пароли на бумажных носителях;
- использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм);
- сохранять пароль автоматически в браузере;
- использовать биографическую информацию в пароле.

Безопасный Wi-Fi:

необходимо:

■ отключить общий доступ к своей Wi-Fi точке, даже если Интернет «безлимитный»;

■ использовать надежный (см.выше) пароль для доступа к Wi-Fi точке;

■ деактивировать автоматическое подключение своих устройств к открытым точкам Wi-Fi;

не рекомендуется:

■ вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

Проверенные браузеры и сайты:

необходимо:

■ использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов;

не рекомендуется:

■ проходить по непроверенным ссылкам;

■ вводить информацию о сайтах, если соединение не защищено (нет https и замка).

Безопасность электронной почты:

необходимо:

■ подключить двух фактурную аутентификацию;

■ использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств защиты) и открытый (для переписки, подписок и т.д.)

■ использовать СПАМ-фильтры;

не рекомендуется:

■ реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники;

■ открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл.

Использование приложений, социальных сетей и мессенджеров:

необходимо:

■ устанавливать приложения только из «PlayMarket», «AppStore» или из проверенных источников;

■ обращать внимание, к каким функциям гаджета приложение запрашивает доступ;

■ обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения;

не рекомендуется:

■ размещать персональную информацию и контактную информацию о себе и открытом доступе;

■ использовать указание геолокации на фото в постах;

■ устанавливать приложения с низким рейтингом и отрицательными отзывами.

Защита данных банковской карты:

необходимо:

■ хранить PIN-код, а также данные для входа в интернет-банк (иные ресурсы) - а именно: пароль, логин, проверочные слова или специальные коды) в безопасном месте, а лучше всего в своей памяти;

■ прикрывать ладонью клавиатуру при вводе PIN-кода;

■ не сообщать третьим лицам данные карты, одноразовые СМС-пароли для подтверждения тех или иных операций;

■ использовать услугу «3D Secure» лимиты на максимальные суммы онлайн-операций;

■ скрыть CVV-код на карте (трехзначный номер на обратной стороне карты), предварительно его сохранив.

не рекомендуется:

■ хранить пин-код вместе с карточкой/на карточке;

■ сообщать CVV-код или отправлять его фото;

■ распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»;

■ сообщать данные, полученные в виде СМС-сообщений, сеансовые пароли, код авторизации, пароль «3D Secure» и т.д.