Материалы

для членов

информационно-пропагандистских групп

(июнь, 2024 г.)

**Современные способы совершения киберпреступлений**

**на территории Витебской области**

*(дополнительная тема)*

В настоящее время киберпреступность представляет серьезную угрозу для развития экономики и общества. За последние годы количество киберпреступлений значительно увеличилось, что требует принятия срочных мер для защиты информации и обеспечения кибербезопасности. Одной из основных проблем является недостаточная осведомленность о кибербезопасности среди населения. Многие граждане не принимают достаточных мер предосторожности при использовании сети Интернет, что делает их уязвимыми перед преступниками.

В 2023 году в Витебской области совершено более 1,5 тысяч киберпреступлений, материальный ущерб составил свыше 2,5 миллионов рублей. Женщины в 2 раза чаще становятся потерпевшими, чем мужчины. Абсолютное большинство проживает в городах. Люди с высшим в равной степени, как и со средним образованием, подвержены обману. Среди жертв киберпреступников, в основном, экономически активные граждане, представляющие практически все сферы деятельности – бухгалтеры, экономисты, директоры, заместители директоров частных и государственных учреждений, начальники управлений и отделов госучреждений, педагоги, врачи и медсестры, студенты, юристы, программисты и представители других специальностей.

Мошенники регулярно меняют свои схемы обмана граждан, чтобы похитить их деньги.

Основными формами обмана являются телефонное мошенничество и фишинговые ресурсы.

**ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО – ВИШИНГ**

Мошенники под видом работников банка или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении. При этом, чтобы войти в доверие, могут выслать фото служебных документов или даже выйти на видеосвязь в мессенджере.

Распространен способ, когда мошенники, используя различные вымышленные ситуации, убеждают потенциальных жертв установить **определенное мобильное приложение**. Оно дает возможность удаленно управлять устройством, на котором установлено. Также злоумышленники убеждают **оформить кредиты в банках**, а деньги перевести на «защищенный» счет.

Мошенники для совершения преступлений изучают свою жертву, собирают в сети Интернет данные о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые сообщения или видеосообщения.

Мошенники регулярно подбирают новые способы обмана, чтобы получить деньги. В сети Интернет размещают рекламу якобы **инвестиционных платформ**, которых на самом деле не существует, чтобы заманить вкладчиков и похитить их деньги. Первым шагом для связи с куратором является заполнение формы, где необходимо оставить свои имя и телефон. Далее с заинтересовавшимся связывается так называемый куратор, под руководством которого в надежде заработать легкие деньги потенциальная жертва сама переводит деньги на электронный кошелек. Чтобы получить хотя бы вложенные деньги обратно, мошенники требуют заплатить комиссии, взносы и т.д. Некоторое время мошенники рисуют жертве их прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на мошеннических счетах.

Чтобы не стать жертвой киберпреступника, как можно раньше закончите разговор с неизвестным лицом, кем бы он не представился.

**ФЕЙКОВЫЕ МАГАЗИНЫ в соцсетях.** Ежедневно в милицию обращаются и те, кто сами перевели **предоплату за товар**, который нашли в объявлениях в социальных сетях и на торговых площадках, и не получили его. Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами (обувь, одежда, мобильные телефоны, постельное белье, новогодние ели, садовые кресла-качалки-коконы и другие товары). Потенциальный покупатель связывается с администратором «магазина», ему обещают доставить товар после полной оплаты. Оплату предлагают произвести на банковскую карту или на счет через ЕРИП. Однако после получения денежных средств, товар не высылают, а покупателя блокируют.

**ФИШИНГ** С целью получения личных данных владельцев счетов мошенники создают страницы-клоны банков, сайтов театров, кальянных и инвестиционных (торговых) бирж.

Для предотвращения подобного необходимо:

* задуматься о причинах низкой цены на товар, отличающейся от цены за тот же товар на сайте или насторожиться почему у магазина нет сайта ;
* тщательно проверять информацию о магазине: связаться с продавцом по белорусскому номеру по мобильной связи, а не через Интернет;
* использовать отдельную карту для расчетов в сети Интернет;
* не переходить по ссылкам от неизвестных вам лиц;
* проверять адрес страницы, где вводите данные карты (для белорусских организаций в адресной строке должно быть так: «название сайта»/BY/«раздел сайта»);
* подключить в настройках карты бесплатную услугу от банка «3-D Secure».

**СВАТИНГ** В молодежной игровой киберсреде распространяется тренд под названием «сватинг». Его суть заключается в том, чтобы создать неблагоприятную обстановку госорганам, нарушить режим их работы, или отомстить своему обидчику, создав для него проблемы с правоохранительными органами.

**ПРЕДПРИЯТИЯ** В области регистрируются киберпреступления, направленные на завладение денежными средствами субъектов хозяйствования, в том числе, государственных предприятий Республики Беларусь.

Хакеры заранее планируют и получают несанкционированный доступ к данным организации, превращают их в беспорядочный набор символов и предлагают расшифровать их после перечисления денежных средств на указанный счет. Злоумышленники прежде всего рассчитывают на человеческие ошибки и слабости, а не на уязвимость программного обеспечения, которую гораздо сложнее преодолеть.

Необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет своевременно выявлена и остановлена, а это возможно на любом ее этапе при принятии соответствующих мер защиты, направленных на сохранение благосостояния, в том числе при соблюдении работниками следующих правил:

1. **обеспечивать должный уровень информационной безопасности** в соответствии с развитием и обновлением программного обеспечения, а также нормативно-правовыми актами Республики Беларусь
2. **регулярно осуществлять резервное копирование** важных данных;
3. **никогда не доверять отправителю электронного письма**, перепроверять указанную информацию, а также основные идентификационные данные и служебные заголовки электронных писем (можно узнать и проанализировать ip-адрес отправителя письма и иную необходимую информацию), прежде чем ответить на письмо, даже если вам пишет давний партнер с нового адреса;
4. **не переходить по ссылкам и не открывать вложения**, если отправитель письма не тот, кем он представился;
5. в случае изменения реквизитов расчетного счета партнера, **устанавливать данный факт по любым другим каналам связи** (лично, по телефону и т.д.);
6. **использовать ключ ЭЦП (электронной цифровой подписи) непосредственно при работе** с соответствующим программным обеспечением, извлекать его из USB-порта после окончания работы;
7. **тщательно проверять адрес сайта;**
8. **своевременно менять пароли к учетным записям**, в том числе при перемещении, увольнении или приеме нового работника;
9. **перепроверять происхождение сайта**, прежде чем ввести персональные данные (адрес, домен, дата создания, реквизиты доступа, финансовые сведения);
10. **немедленно сменить пароль и(или) заблокировать счета** в случае введения реквизитов доступа на подозрительном сайте;
11. **всегда быть бдительным** и проверять полученную информацию.