Обеспечение безопасности осуществления платежей в сети Интернет

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.

По статистике 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 и интернет-мошенничество, а также фишинговые ресурсы.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО – ВИШИНГ

Мошенники под видом работников банка, операторов связи 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 загрузить направленный в мессенджере файл или установить определенное мобильное приложение. В обоих случаях мошенники получают возможность удаленно управлять устройством, на котором установлено. Таким образом они получают доступ к личным данным пользователей, в том числе имеют возможность оформить онлайн-кредит. Также злоумышленники убеждают оформить кредиты в банках, а деньги перевести на «защищенный» счет.

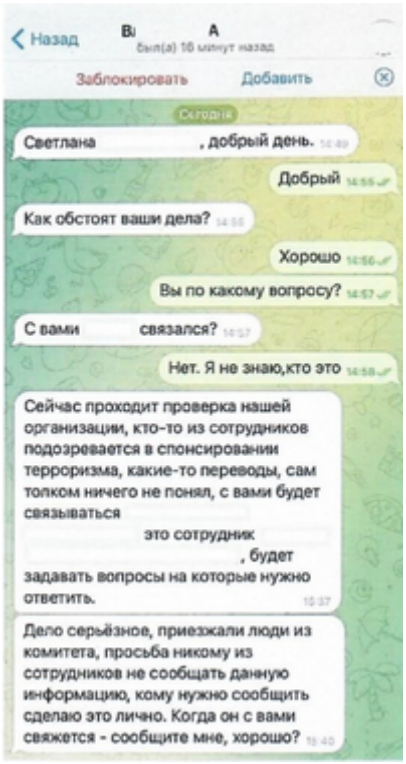
Всегда надо быть начеку и не доверять незнакомым, ни под каким предлогом не устанавливать непроверенные программы и файлы, полученные в мессенджере от неизвестных, не передавать кому бы то ни было деньги и не переводить их на банковские счета по указанию незнакомых.

В Орше в течение нескольких дней женщине звонили с незнакомых номеров. В конечном итоге она согласилась выслушать псевдоследователя. Он ошарашил ее тем, что с ее счета фиксируются незаконные операции на мошеннические счета и необходимо их предотвратить и установить злоумышленников. Женщина отказывалась верить ему, тогда с ней продолжил беседу по видеосвязи якобы работник одного известного банка, который был в деловой форме одежды с атрибутами банка. Женщина поверила звонившим и по их рекомендации установила приложение, которое позволило мошенникам видеть все происходящее на ее телефоне, в том числе смс-коды. В разговоре с лжебанкиром она назвала кодовое слово – девичью фамилию матери, а уже сообщники мошенников воспользовались этим и оформили на женщину овердрафт и онлайн-кредит прямо во время разговора и перевели их на свои счета. Всего у женщины похитили 18 тысяч рублей.

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 текстовые или видеосообщения.

Например, в мае зарегистрировано несколько подобных фактов. В мессенджере мошенники создали учетную запись руководителя госорганизации и от его имени написали сотруднице, что поступили списки работников, которые подозреваются в финансировании экстремистских формирований, и вскоре, возможно, в жилье женщины проведут обыск и изымут незадекларированные денежные средства. Женщина очень испугалась за свои деньги, потому

что доверяла руководителю. Далее мошенники от имени ее руководителя предложили пообщаться с Начальником Департамента финансовых расследований области, который в свою очередь связал ее со следователем. В течение трех дней женщина пребывала в страхе за свои сбережения. Чтобы сохранить их мошенники «посоветовали» перевести их на якобы специальный защищенный счет. Также женщина за неделю получила кредит, обналичила его и перевела на тот же счет. откуда вскоре все деньги в сумме 55 тысяч были похищены.



Аналогичные случаи зафиксированы в отношении педагогических работников области, мошенники в мессенджере писали от имени директоров учебных заведений. Более 7 педагогов обратились в милицию в течение 3 дней, некоторые обращались позже. В основном, мошенники убеждали учителей получить кредиты в банках.

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.

Молодой витебчанин заинтересовался возможностью вложить свои деньги в инвестиционный проект. После того как он выполнил указания куратора и перевел деньги на цифровой кошелек, сумма его денег стала якобы увеличиваться, в своем аккаунте на платформе молодой человек видел прибыль, однако, как только он попытался вывести деньги, его сразу же заблокировали. Он дважды находил в интернете фирмы по оказанию помощи по выводу денег, однако ни одна «фирма» ему не оказала должных услуг, после чего мужчина обратился в милицию. Всего он потерял более 20 тысяч рублей.

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.

Молодая мама из Орши, находящаяся в декретном отпуске, перевела на предоставленный счет через ЕРИП 2 тысячи рублей за телефон, но не получила его. Тогда мошенники предложили ей получить свои деньги обратно на банковскую карту. Они направили в мессенджере ссылку, перейдя по которой, девушка ввела в ячейки номер карты и секретный код с оборотной стороны, предназначенный только для расходных операций. Завладев этими сведениями, мошенники обманули ее еще раз, списав с карты все деньги.

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;

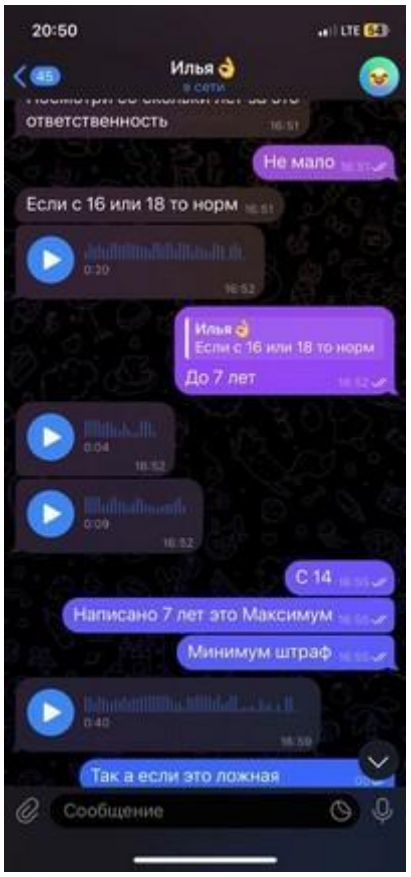
• проверять адрес страницы, где вводите данные карты (для белорусских организаций в адресной строке должно быть так: «название сайта».BY/«раздел сайта»);

• 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. За первое полугодие 2024 года в области выявлено 4, а за предыдущие 2 года – восемь школьников, которые организовывали рассылку писем на электронные почтовые ящики организаций Беларуси и других стран с ложными сообщениями о заминировании объектов.

Все установленные лица – несовершеннолетние, самому младшему сватеру 12 лет, все они намеренно использовали методы деанонимизации и специальное программное обеспечение, как они думали, позволяющее скрыть следы. Подростки интересовались темой сватинга и в большинстве случаев знали, что за совершение данных деяний уголовная ответственность наступает с 14 лет и предусматривает вплоть до 7 лет лишения свободы.



ВОВЛЕЧЕНИЕ В КИБЕРПРЕСТУПНОСТЬ

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных лиц, так называемых «дропов». Часто промежуточных счетов бывает более десятка. Имеются факты, когда полученные незаконным путем деньги проходили через 72 промежуточных банковских счета, доступ к которым мошенники покупали у их владельцев.

В нашей стране открыть банковский счет может дееспособный гражданин с 14 лет, то есть даже несовершеннолетние могут открыть банковские счета. Этим целях пользуются преступники. Находясь за границей, злоумышленники подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет в интернет-банкинге, а также предоставить разовый смс-код или карту кодов.

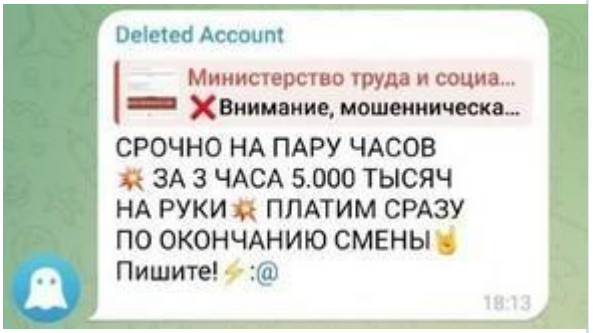
Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда или людей для разгрузки товаров, или людей на вакансию «тайный покупатель», или заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Ответственность за возникновение прошедших по банковским счетам денег несут владельцы таких счетов.

Надо знать, что в нашем законодательстве статьей 222 Уголовного кодекса предусмотрена ответственность вплоть до 10 лет лишения свободы за изготовление в целях сбыта либо сбыт банковских платежных карт или иных платежных инструментов, таких как банковские счета или электронные кошельки, а также распространение данных доступа к ним.
Имеются факты, когда в преступную деятельность были вовлечены несовершеннолетние.
16 подростков из двух учреждений среднего специального образования области, связавшись с заказчиком из Интернета, оформляли на свое имя банковские карты и за вознаграждение от 15 до 50 рублей передавали их для использования неустановленным лицам. С использованием этих банковских карт киберпреступники переводили похищенные деньги. В отношении 8 подростков возбуждены уголовные дела, в отношении остальных – проводится проверка и решается вопрос о возбуждении уголовных дел.
Кроме этого, имеются примеры вовлечения подростков в преступную цепочку другим способом.
14-летний ученик Витебской школы попросил на некоторое время в пользование у своего 15-летнего одноклассника его банковскую платежную карту. Парень зарегистрировал аккаунт на криптовалютной бирже. Неизвестные лица связались с ним и предложили заработать. Молодой человек предоставил реквизиты банковской карты одноклассника, на которую он получил 10 000 рублей, а после чего для них купил криптовалюту на всю сумму. В ходе проверки установлено, что полученные деньги были похищены у пенсионера из Витебска.
Таким образом, школьник оказал услуги по покупке-продаже криптовалюты третьим лицам, что влечет ответственность за незаконную предпринимательскую деятельность по ч.3 ст. 13.3 КоАП Республики Беларусь. Совершение сделок на криптовалютной бирже подростками – не единичный случай. Через криптокошелек другого подростка прошло более 450 тысяч рублей.
За совершение сделок с криптовалютой в пользу третьих лиц грозит крупный штраф и обращение в доход государства до ста процентов суммы дохода, полученного в результате такой деятельности.
Приложение: листовка об ответственности





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 и домен сайта, дата его создания;
8. своевременно менять пароли к учетным записям, в том числе при перемещении, увольнении или приеме нового работника;
9. немедленно сменить пароль и(или) заблокировать счета в случае введения реквизитов доступа на подозрительном сайте;
10. всегда быть бдительным и проверять полученную информацию.

Управление по противодействию киберпреступности
КМ УВД Витебского облисполкома