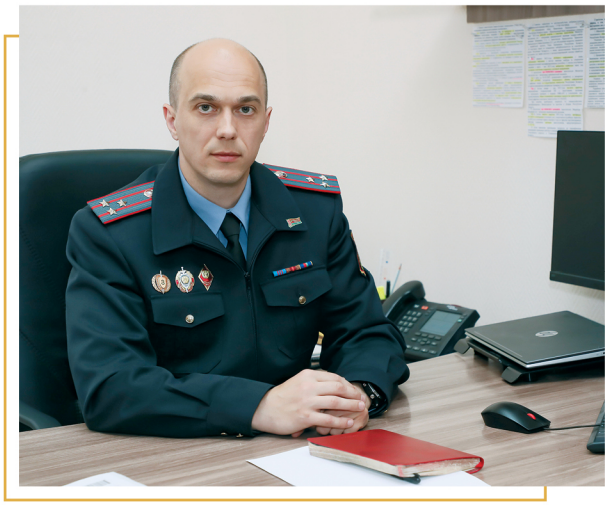
ИГРА НА ДОВЕРИИ, СТРАХЕ И ЖАДНОСТИ

В Беларуси ежегодно тысячи граждан становятся жертвами киберпреступлений. Сегодня киберпреступники стали изощреннее: они играют на доверии, страхе и жадности, используя социальные сети, фишинг и даже искусственный интеллект.

Какие схемы сейчас наиболее опасны? Как защищают граждан от мошенников и почему даже «период охлаждения» при выдаче кредитов может спасти от потери денег? Об этом рассказал заместитель начальника главного управления по противодействию киберпреступности МВД Беларуси Александр РИНГЕВИЧ.



ЭВОЛЮЦИЯ КИБЕРПРЕСТУПЛЕНИЙ

ВС

– Сегодня вопросы кибербезопасности находятся в ведении нескольких госструктур: Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства внутренних дел, Следственного комитета... Какие задачи сегодня выполняет главное управление по противодействию киберпреступности МВД?

– Наша работа строится в двух направлениях: реактивном и превентивном. Первостепенная задача специалистов главного управления – **защита прав граждан**, уже ставших жертвами киберпреступлений: раскрытие преступлений, поиск злоумышленников и помощь в возврате похищенных средств. Параллельно мы ведем **анализ причин и условий**, способствующих совершению преступлений, чтобы предотвратить их повторение. Это включает как точечные меры – например, препятствование распространению схем мошенничества, так и системные изменения, в том числе на законодательном уровне. Ну и особое внимание – **профилактической работе**.

ВС

– За чем сегодня охотятся цифровые мошенники? И как часто меняются сценарии атак?

– 90% преступлений по нашему направлению служебной деятельности – это преступления, связанные

с противоправным получением денежных средств путем мошенничества, хищения или вымогательства. Остальные 10% – иные преступления (например, ложные сообщения об опасности, получение несанкционированного доступа к компьютерной информации, неправомерное распространение средств платежа).

Надо понимать: современные киберпреступления – это симбиоз старых приемов манипуляции доверием и новых технологических возможностей с целью наживы. Злоумышленники охотятся либо напрямую за денежными средствами граждан, либо за их конфиденциальной информацией, чтобы впоследствии использовать ее в своих преступных схемах.

Еще лет 5 назад злоумышленники действовали по примитивному шаблону – банально звонили и просили реквизиты банковской карты, включая номер, срок действия и CVC-код. Сегодня же их приемы стали куда более замысловатыми. Применяемые сценарии регулярно обновляются: средняя «продолжительность жизни» сценария – 3 – 6 месяцев. Хотя есть и уже ставшие классическими. Например, продаже несуществующих товаров.

– Теперь – к вопросу о новых технологиях. Сегодня, когда речь заходит о развитии искусственного интеллекта, в первую очередь говорят о рисках его использования мошенниками. Так как часто ИИ действительно применяется в преступных схемах?

– Искусственный интеллект преступники в своих схемах пока используют не часто: методы с его применением требуют индивидуального подхода к каждой жертве и тщательной подготовки. Гораздо проще продолжать использовать традиционные схемы, которые работают на массовую аудиторию, без необходимости подстраиваться под каждого конкретного человека.

Тем не менее появление доступных инструментов на основе ИИ уже меняет ландшафт киберпреступности. Эти технологии стали настолько доступными и эффективными, что сегодня даже неопытный злоумышленник без специальных знаний программирования может создать фальшивое видео или аудио, используя общедоступные и относительно недорогие инструменты.

ИИ применяется в мошеннических схемах прежде всего для создания дипфейков. Злоумышленники делают поддельные видео, где якобы знаменитость или авторитетный человек рекомендует какую-то инвестиционную схему или компанию. Такие подделки выглядят настолько убедительно, что могут ввести в заблуждение даже осторожных пользователей.

Современные киберпреступления – это симбиоз старых приемов манипуляции доверием и новых технологических возможностей с целью наживы. Злоумышленники охотятся либо напрямую за денежными средствами граждан, либо за их конфиденциальной информацией, чтобы впоследствии использовать ее в своих преступных схемах.

Опасным трендом стало использование ИИ для создания поддельных голосовых или видеосообщений. Как правило, после взлома аккаунта и получения доступа к переписке в мессенджерах, мошенники находят настоящее голосовое или видеосообщение-кружок жертвы, загружают его в специальную программу, а затем генерируют любое новое сообщение голосом этого человека. Такой механизм используют для создания убедительных просьб о срочной финансовой помощи, которые сложно отличить от настоящих. Например: *«Привет, у меня не получается говорить, стою на трассе, срочно нужны деньги на эвакуатор, переведи по таким-то реквизитам»*. Такие сообщения рассылаются по всему списку контактов.

Искусственный интеллект мошенники в своих схемах пока используют не часто: методы с его применением требуют индивидуального подхода к каждой жертве и тщательной подготовки. Гораздо проще продолжать использовать традиционные схемы, которые работают на массовую аудиторию, без необходимости подстраиваться под конкретного человека.

АТАКИ НА БИЗНЕС

– Кибермошенники против бизнеса: каким образом и как часто атакуют компании?

– В общем числе пострадавших от киберпреступлений, зафиксированных в Беларуси, доля юрлиц – не более 5%. Для проведения атак на юридические лица злоумышленникам приходится прикладывать гораздо больше усилий, и даже при тщательной подготовке успех не всегда гарантирован.

Основных проблем, с которыми сталкиваются юрлица, две. Первая – это **несанкционированный доступ к служебной информации, базам данных**. Мошенники либо взламывают корпоративную почту, либо создают ее копию с едва заметными изменениями (например, заменяют одну букву в адресе). Затем они имитируют переписку с контрагентами и подменяют реквизиты платежей. Вторая распространенная проблема – это **проникновение вредоносного ПО, которое шифрует данные,** с последующим требованием выкупа. Такие программы часто попадают в систему через вложения в электронных письмах или уязвимости в программном обеспечении.

В последние годы количество успешных атак на компании сокращается. Это связано с усилением контроля за международными переводами, появлением в организациях служб информационной безопасности и более внимательным отношением банков к подозрительным операциям.

Принципиальное отличие атак на компании заключается в их сложности. Если для обмана физического лица достаточно изучить его профиль в соцсетях и грамотно построить беседу, то с юридическими лицами все иначе. Здесь нужно преодолеть несколько уровней защиты: изучить переписку, понять систему и определить уровни принятия решений, обойти возможные проверки со стороны банков. Даже при успешной атаке есть риск, что подозрительный перевод будет заблокирован или сотрудники компании вовремя заметят подвох.

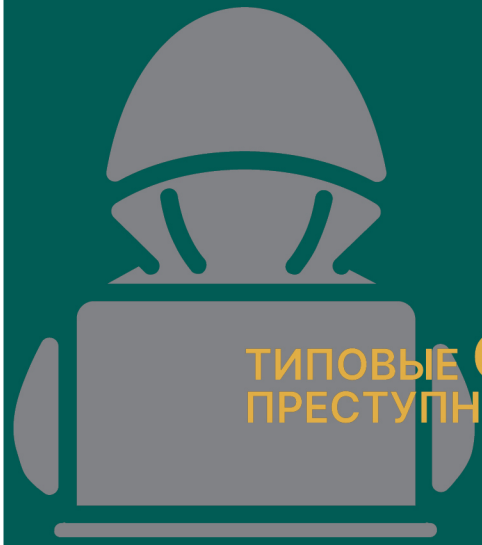
Любопытно, что во многих случаях атак на юрлиц злоумышленники даже не выбирают конкретную жертву заранее. Вредоносное ПО распространяется массово, и его жертвой может стать как небольшой ИП с одной торговой точкой, так и крупное предприятие. Размер требуемого выкупа тоже определяется случайным образом: для одних компаний он может быть незначительным, для других – совершенно неподъемным.

В последние годы количество успешных атак на компании сокращается: это связано с усилением контроля за международными переводами, принятием организациями технических мер защиты информации и более внимательным отношением банков к подозрительным операциям.

– Вы отметили, что одна из целей преступников – базы данных с конфиденциальной информацией. Как обычно злоумышленники распоряжаются этими сведениями?

– Когда злоумышленники получают доступ к базам данных компаний, эта информация превращается в товар на черном рынке. Ценность таких баз зависит от их содержания: это могут быть клиентские списки торговых сетей, логины и пароли от личных кабинетов, банковские реквизиты или даже копии документов. Чем полнее и «свежее» данные, тем выше их цена.

Но даже фрагментарная информация – старые адреса, номера телефонов, электронные почты – представляет интерес для мошенников. Все это используется в социальной инженерии: звонки с угрозами, фишинговые рассылки, поддельные просьбы о помощи. Например, если в базе есть связка «почта + пароль», злоумышленники проверяют ее на популярных сервисах – вдруг человек использовал один и тот же пароль везде?



ТИПОВЫЕ СЦЕНАРИИ ПРЕСТУПНЫХ СХЕМ

ПОДДЕЛЬНЫЕ ИНТЕРНЕТ-БАНКИНГИ, РЕСУРСЫ ДЛЯ ОПЛАТЫ ИЛИ ПЕРЕВОДА СРЕДСТВ

Данные (например, реквизиты банковских карт, логины, пароли), введенные на фишинговых ресурсах, сразу же попадают в руки мошенников и впоследствии используются в преступных схемах.

«ПОМОЩЬ ДРУГУ»

Через взломанные аккаунты мошенники пишут от имени жертвы ее родным и знакомым о срочной просьбе одолжить деньги или поучаствовать в опросе по приведенной ссылке. Откликнувшись на такой запрос, жертва в первом случае сама переводит мошенникам средства, во втором – предоставляет им доступ к своей конфиденциальной информации.

«ДЕКЛАРИРОВАНИЕ СРЕДСТВ» ПО ЗВОНКУ

Мошенники сначала представляются сотрудниками правоохранительных органов и сообщают, что проводится проверка, а деньги гражданина якобы участвуют в незаконных операциях. После этого звонок «переводят» на мнимого сотрудника банка, который под тем же предлогом просит перевести средства на «защищенный счет» или диктует код из SMS, будто для отмены подозрительной операции, а на самом деле – для доступа к интернет-банкингу.

«ВЫГОДНЫЕ» ПРЕДЛОЖЕНИЯ НА «ДОСКАХ ОБЪЯВЛЕНИЙ»

Самая распространенная схема в соцсетях и группах мессенджеров (примерно 40% от числа всех киберпреступлений). Мошенники завлекают граждан под видом продажи вещей, билетов, аренды квартир, цены на которые ставят обычно ниже рыночных, что и привлекает многих. Покупатель сам связывается с продавцом-мошенником, тот просит предоплату на карту или через перевод и после получения денег, как правило, исчезает.

ПОДДЕЛЬНЫЕ ПЛАТФОРМЫ ДЛЯ ИНВЕСТИРОВАНИЯ

Гражданам, зачастую посредством таргетированной рекламы, предлагают сделать «выгодные» инвестиции в криптовалюту, акции, другие активы. Люди, как правило, слабо разбирающиеся в вопросе, переводят мошенникам крупные суммы. Причем делают это зачастую неоднократно и даже берут для этого кредиты. Чтобы вызвать доверие у людей, мошенники создают сайты с поддельными логотипами, отзывами и даже могут временно позволять выводить небольшие суммы. Но после попытки забрать все деньги «кураторы» перестают выходить на связь, сайты исчезают.

ЗВОНКИ ОТ ИМЕНИ ОПЕРАТОРОВ СВЯЗИ

Мошенники сообщают, что договор на услуги требует срочного продления, и просят перейти по ссылке из SMS или назвать конфиденциальную информацию. Иногда жертву вовлекают в многоходовую аферу: сначала убеждают, что ее деньги «в опасности», затем предлагают поучаствовать в «спецоперации» – съездить к другим людям, забрать у них средства и перевести на «безопасный счет». В результате человек не только теряет свои деньги, но и невольно становится посредником в мошенничестве.

Преступники всегда применяют психологическое давление: создают ощущение срочности, угрожают блокировкой счетов или предлагают «единственный способ» решить проблему. Все сценарии – это игры на доверии, страхе и жадности.

ОТВЕТ НА УГРОЗЫ

– Могут ли правоохранители повлиять на распространение украденных данных?

– Главная проблема утечек данных заключается в том, что полностью изъять украденные сведения из оборота практически невозможно. Площадки в даркнете, где распространяется такая информация, специально создаются анонимными, с использованием технологий, скрывающих их реальное местоположение и владельцев. Даже если удается заблокировать один такой ресурс, данные моментально появляются на других. Потому мы фокусируемся на минимизации последствий утечек и предотвращении их дальнейшего использования злоумышленниками.

Лимиты на переводы, обязательные подтверждения операций, задержки в проведении подозрительных платежей... – все это несильно усложняет жизнь обычным гражданам, но создает серьезные препятствия для мошенников. Как показывает практика, даже 24 часа – достаточный срок, чтобы потенциальная жертва успела опомниться, а преступник – остаться ни с чем.

Когда происходит утечка данных, обычно организуется массовая смена компрометированных сведений. Если в украденной базе содержатся логины и пароли какого-либо ресурса, то пользователям рассылаются уведомления о необходимости срочно изменить свои учетные данные. Этот подход делает украденную информацию практически бесполезной для злоумышленников, так как доступ к аккаунтам блокируется.

Параллельно банкам направляются списки клиентов, чьи данные могли быть скомпрометированы, чтобы они усилили мониторинг их финансовых операций. Современные системы аналитики банков позволяют выявлять подозрительную активность – например, когда после оформления банковской карты на территории Беларуси или с белорусских IP-адресов спустя короткий промежуток времени поступает запрос на снятие денежных средств в другой стране. В таких случаях счета оперативно блокируются для предотвращения мошеннических операций.

– Какие еще принимаются меры, чтобы обезопасить граждан?

– Чуть больше года назад был принят Указ Главы государства «О мерах по противодействию несанкционированным платежным операциям», которым было закреплено взаимодействие по обмену информацией о несанкционированных платежных операциях между правоохранительными органами и поставщиками платежных услуг. И сегодня этот механизм отлажен до мелочей. Например, когда пенсионерка из глубинки подает заявление о мошенничестве, информация мгновенно поступает в специальный отдел МВД. Там оперативно проверяют данные и передают их поставщикам платежных услуг, которые начинают собственное расследование: отслеживают цепочку перемещения денег, блокируют подозрительные счета и приостанавливают операции. Пока мошенники пытаются вывести средства через цепочку счетов, правоохранители уже блокируют расходные операции. Весь процесс занимает даже не часы – минуты. Работа ведется в режиме 24/7. К слову, в данный момент этот же механизм берет на вооружение и Российская Федерация.

Сегодня у нас в принципе особая роль отводится банковским департаментам безопасности: они не только реагируют на инциденты, но и предотвращают их. Например, если пенсионер пытается перевести крупную сумму на подозрительный счет, система может автоматически заблокировать операцию и потребовать личного визита в отделение. Это создает «барьер времени» – возможность одуматься или получить консультацию.

Еще одна мера – введенный пару лет назад «период охлаждения» при оформлении кредитов. Раньше мошенники заставляли жертв брать займы и тут же переводили деньги на свои счета. Теперь между подачей заявки и выдачей денег проходят сутки – срок, за который многие успевают понять, что стали жертвами обмана. Сокращение числа тяжких в сфере киберпреступлений на 15% может косвенно свидетельствовать о том, что мера работает.

Поскольку организаторы киберпреступлений обычно находятся за рубежом, основная работа ведется с местными пособниками – теми, кто оформляет подставные банковские карты, снимает наличные или переводит средства.

Когда мошенники стали использовать криптовалюты для отмывания денег, было введено жесткое регулирование оборота цифровых активов. Тем самым закрыты лазейки для мошеннических схем недобросовестных криптовалютчиков.

Лимиты на переводы, обязательные подтверждения операций, задержки в проведении подозрительных платежей... – все это несильно усложняет жизнь обычным гражданам, но создает серьезные препятствия для мошенников. Как показывает практика, даже 24 часа – достаточный срок, чтобы потенциальная жертва успела опомниться, а преступник – остаться ни с чем.

– Насколько реально сегодня вычислить киберпреступника и привлечь его к ответственности?

Главное отличие киберпреступлений от, скажем так, традиционных видов преступной деятельности в том, что они носят трансграничный характер: злоумышленникам не нужно физически находиться в стране, против граждан которой они совершают противоправные действия. Современные технологии позволяют организовывать атаки из любой точки мира, и это создает серьезные сложности для правоохранительных органов.

Сейчас основная масса, например, кол-центров, специализирующихся на мошеннических звонках под видом сотрудников банков или правоохранительных органов, сосредоточена на территории Украины. Там подобная деятельность ведется практически открыто – набор сотрудников проводится через публичные объявления, а сами преступники не особо скрывают свою деятельность. Это стало возможным из-за слабого противодействия со стороны местных правоохранительных органов. При этом украинские кол-центры активно используют пособников в других странах, в том числе и у нас, для непосредственного вывода денежных средств.

Расследование таких преступлений – сложный многоэтапный процесс. Поскольку организаторы находятся за рубежом, основная работа ведется с местными пособниками – теми, кто оформляет подставные банковские карты, снимает наличные или переводит средства. Несмотря на объективные трудности нынешнего времени, ведется работа и по установлению зарубежных организаторов. Следственные органы собирают доказательную базу, объявляют таких лиц в международный розыск, хотя реальная возможность их задержания и остается ограниченной. При этом активно развивается международное сотрудничество, особенно с правоохранительными органами России и Казахстана, где наблюдается схожая картина преступлений.

– Вы отмечали, что одно из направлений работы по противодействию киберпреступности – профилактика. Очевидно, в этом направлении вы говорите людям, как не стать жертвой мошенников. А упоминаете ли вы, как не стать участником мошеннических схем? Как сегодня выстраивается профилактическая работа?

– В своей профилактической работе мы особое внимание уделяем работе с молодежью. Этой категории граждан как раз не только объясняют, как не стать жертвой, но и рассказывают об ответственности за соучастие в преступлениях. Ведь многие ребята, соблазнившись «легкими деньгами», даже не осознают, что помогают мошенникам, – для них это абстрактные «операции», а не кража у реальной бабушки-пенсионерки. Так как классические методы правового просвещения с молодежью практически не работают, для них разрабатываются специальные квесты и интерактивные форматы. Один из самых ярких примеров – проект «Киберкрепость» в Telegram, запущенный управлением по противодействию киберпреступности УВД Брестского облисполкома и ставший образцом для других регионов. Его особенность – неформальный подход к подаче информации.

Современные технологии позволяют организовывать атаки из любой точки мира, и это создает серьезные сложности для правоохранительных органов. Сейчас основная масса, например, кол-центров, специализирующихся на мошеннических звонках под видом сотрудников банков или правоохранительных органов, сосредоточена на территории Украины.

Надо понимать: профилактика сегодня – это не скучные лекции о новых мошеннических схемах, а постоянный диалог с обществом. И хотя идеальной защиты от мошенников не существует, в том числе такие меры помогают тысячам людей не потерять свои деньги – развивают критичность мышления. А сегодня это самое главное оружие в борьбе с киберпреступностью. ВС

Анастасия МАНУИЛОВА