Учреждение образования
«Гродненский государственный университет имени Янки Купалы»

ПАМЯТКА
по профилактике преступлений (правонарушений) в сфере информационной безопасности и недопущению хищений посредством сети Интернет

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз; сохранение конфиденциальности, целостности и доступности информации в киберпространстве, а также защищенности информационной инфраструктуры.

Киберпреступление – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.).

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

ст. 209 «Мошенничество»;

ст.212 «Хищение имущества путем модификации компьютерной информации»;

ст.349 «Несанкционированный доступ к компьютерной информации»;

ст.350 «Уничтожение, блокирование или модификация компьютерной информации»;

ст.352 «Неправомерное завладение компьютерной информацией»;

ст.354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»;

ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»

Основными формами обмана являются телефонное и интернет-мошенничество, а также фишинговые ресурсы.

ФИШИНГ (англ. phishing от fishing «рыбная ловля, выуживание») – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.).

С целью получения личных данных владельцев счетов мошенники создают страницы-клоны сайтов банков, 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 на сайте указаны другие цены;

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 (проверить подключение) в настройках карты бесплатную услугу от банка «3-D Secure» – это дополнительная защита от банка, которая предлагает ввести код, пришедший в смс-сообщении.

ВИШИНГ (англ. vishing – voice + phishing) – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.

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!

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.

Публичность, доступность и анонимность – благоприятная почва для киберпреступности!

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

ИНВЕСТИЦИОННЫЕ ПЛАТФОРМЫ

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 прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на счетах мошенников.

ФЕЙКОВЫЕ МАГАЗИНЫ в соцсетях

Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами (обувь, одежда, мобильные телефоны, постельное белье, автомобильные шины, новогодние ели, садовые кресла-качалки-коконы и другие товары). Потенциальный покупатель связывается с администратором «магазина» и обещает доставить товар после частичной или полной оплаты. Перевод денег предлагают произвести на банковскую карту или на счет через ЕРИП, что притупляет бдительность. После получения денежных средств, Интернет-магазин товар не высылает, а покупателя блокирует.

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. Чаще всего установленные лица – несовершеннолетние.

Подростки интересовались темой сватинга и в большинстве случаев знали, что за совершение данных деяний уголовная ответственность наступает с 14 лет и предусматривает наказание 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. В Республике Беларусь открыть банковский счет может дееспособный гражданин с 14 лет, то есть даже несовершеннолетние могут открыть банковские счета. Этим в своих 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. 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 происхождение прошедших по банковским счетам денег несут владельцы таких счетов.

Надо знать, что в законодательстве Республики Беларусь 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.

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.

ОПЕРАЦИИ С КРИПТОВАЛЮТОЙ

Указом Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)» (далее – Указ № 367) установлена обязанность для физических лиц совершать операции по покупке-продаже криптовалюты за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий, а также перечислять (переводить) денежные средства со своих банковских счетов, электронных кошельков исключительно указанным резидентам ПВТ. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается.

Разрешено: покупать токены (криптовалюту) за денежные средства только на белорусских криптобиржах, являющихся резидентами Парка высоких технологий; обменивать токены на другие токены на любых криптоплатформах без ограничений, например, обменивать Bitcoin на Ethereum.

Запрещено: покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах.

Не попадитесь на уловки мошенников!

Помните:

Представители правоохранительных органов, государственных организаций НИКОГДА НЕ ЗВОНЯТ на МЕССЕНДЖЕРЫ! (исключения, если Вы сами дали свой номер для связи сотруднику и знаете его лично);

ни под каким предлогом не сообщайте по телефону персональные (паспортные) данные, номера банковских карт или одноразовые пароли, пришедшие Вам на мобильный телефон;

приложение мобильного оператора можно скачивать только из магазинов «Google Play», «App Store», «App Gallery», а не с направленных Вам ссылок на сайты незнакомыми лицами;

никогда не оформляйте кредиты по просьбе или требованию третьих - не проводите через банкоматы, а также системы банковского обслуживания сети Интернет, никакие денежные операции по инструкциям, полученным по телефону или мессенджеру.

Если поступил сомнительный звонок, незамедлительно завершите разговор и обратитесь в милицию по номеру «102».

Наиболее актуальные преступные схемы:

1. Поступает звонок в мессенджере (Telegram, Viber), звонивший представляется:

- милиционером, следователем (сотрудником других правоохранительных органов), Вас пытаются убедить:

родственник, иной близкий человек, спровоцировал ДТП, для избежания уголовной ответственности необходимо срочно передать через курьера денежные средства пострадавшему;

поучаствовать в операции по разоблачению преступников, оформивших кредит на Ваше имя, для чего перечислить Ваши деньги на «безопасный» счет, либо оформить кредит (для дистанционной помощи сообщить Ваши персональные данные, код пришедший на телефон);

- сотрудником банка, представителем операторов сотовой связи, домашней телефонии, провайдера сети Интернет (РУП «Белтелеком» и д.р.), Вас пытаются убедить:

передать (перечислить) Ваши деньги представителю банка для их декларирования;

перезаключить (обновить) договоры услуг (мобильной/стационарной связи, доступа к сети Интернет и д.р.), перейдя по направленной мошенником ссылке для установки приложения (помните, договоры на оказания таких услуг как правило бессрочны);

2. Реклама в сети Интернет, предлагающая вложить (использовать) Ваши накопления с доходом на «крайне выгодных» условиях (инновационные средства заработка, заработок на бирже, приобретение криптовалюты, вложения средств с повышенной доходностью по счетам и вкладам).

3. Приобретение в сети Интернет товаров по цене ниже рыночной, в т.ч. перечисление предоплаты в адрес продавца для его брони.

4. Сообщения (реклама, звонок) о выигрыше в лотерее (ином розыгрыша) с условием, что для его получения необходимо предварительно перечислить деньги.

Будьте бдительны! Эти знания помогут спасти Ваши деньги!