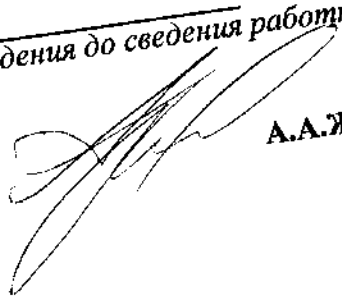
Каменецкий районный исполнительный комитет
Управляющий делами райисполкома

Срок исполнения:

Руководителям структурных подразделений
Председателям горсельисполкомов
Служба «Одно Окно»

Для доведения до сведения работников



А.А.Жукович

10.03.2023

УПРАЎЛЕННЕ ЎНУТРАННЫХ СПРАЎ
БРЭСЦКАГА АБЛАСНОГА
ВЫКАНАЎЧАГА КАМІТЭТУ

АДДЗЕЛ УНУТРАННЫХ СПРАЎ
КАМЯНЕЦКАГА РАЁННАГА
ВЫКАНАЎЧАГА КАМІТЭТУ

вул. 8 Сакавіка, д. 1,225051, гор. Камянец
тэл. (01631) 7 50 48, факс 7 50 13
E-mail: rovd_kamenets@mvd.gov.by

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ
БРЕСТСКОГО ОБЛАСТНОГО
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

ОТДЕЛ ВНУТРЕННИХ ДЕЛ
КАМЕНЕЦКОГО РАЙОННОГО
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

ул. 8 Марта, д. 1,225051, гор. Каменец
тел. (01631) 7 50 48, факс 7 50 13
E-mail: rovd_kamenets@mvd.gov.by

06.03.2022 года исх.№ 51/40/1435

Председателю
Каменецкого райисполкома
Кулаку В.В.

О направлении информации

Направляю в Ваш адрес профилактическую информацию для доведения всем субъектам профилактики в сфере высоких технологий.

Приложение: информационное письмо на 3 листах.

Начальник
Каменецкого РОВД В.А. Водчиц

51/40/2, Юзвук, 76287
М.В., 06.03.2023

Для доведения до сведения!

Повсеместное внедрение и использование компьютерных информационных технологий, безусловно, создает возможности для более эффективного развития экономики, политики, общества и государства в целом. Однако совершенствование и применение высоких технологий приводит не только к укреплению информационного общества, но и появлению новых угроз, одной из которых является компьютерная преступность.

Рассмотрим основные угрозы, которым подверглись жители Каменецкого района за прошедший 2022 год и методы защиты от них.

1. ВИШИНГ

Вишинг – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

В большинстве случаев при совершении звонков потерпевшим преступники используют IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

Справочно: на территории Каменецкого р-на за 2022 год зафиксировано 12 фактов мошенничества путем вишинга, общая сумма похищенных средств составила 29, 249 рублей.

2. ФИШИНГ

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т. д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

Справочно: на территории Каменецкого р-на за 2022 год зафиксировано 12 фактов мошенничества путем фишинга, общая сумма похищенных средств составила 12, 869 рублей.

Вместе с тем, на территории Каменецкого района был зафиксирован 1 факт хищения денежных средств жительницы района ввиду «неочевидного» фишинга. 21.09.2022 жительница аг. Беловежский используя сеть «Интернет», зашла через браузер на поддельный сайт банковского учреждения, клиенткой которого является. Фишинговый ресурс визуально был идентичен официальному сайту банка, однако в поисковой строке вместо официального адреса, например: «belarusbank.by», были указаны иные значения: «stardraft.store». Войдя в свой кабинет и введя данные своей платежной карты гражданка лишилась 306 рублей.

14.01.2023 также зафиксирован аналогичный факт на территории Каменецкого района, сумма ущерба составила 700 рублей.

3. МОШЕННИЧЕСТВО В СОЦСЕТЯХ

В настоящее время особо актуальной становится проблема защиты аккаунтов в социальных сетях и противодействия различным формам и видам мошенничества. Наиболее типичные способы обмана в соцсетях сегодня таковы:

Предоплата

Злоумышленники размещают объявления о продаже каких-либо товаров по бросовым ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

Справочно: за 2022 год посредством соц. сети «Instagram» под видом онлайн-магазинов по продаже цветов, мужской/женской одежды, бытовой мебели было зафиксировано 12 фактов хищения средств жителей Каменецкого р-на, общая сумма похищенных средств составила 2, 629 рублей. Остальные 11 фактов совершены на kufar.by, Telegram, ВКонтакте, иных сайтах.

Шантаж и вымогательство

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

Справочно: за 2022 год зафиксирован 1 факт указанной категории. 15.05.2022 житель Каменецкого р-на при заказе интим-услуг перевел злоумышленнику предоплату. После получения денежных средств злоумышленник под предлогом разглашения факта заказа услуг родным молодого человека, а после используя угрозы применения

насилия в отношении последнего и его родных вымогали дополнительных переводов денежных средств. Общая сумма похищенных средств составила 890 рублей.

Онлайн-игры, трейдинг

Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги. Также популярны услуги «профессиональных» трейдеров. Непосредственная работа трейдера: анализ текущей ситуации на рынке и заключение торговых сделок, т.е. будущий потерпевший переводит свои денежные средства «трейдеру», который обещает удвоить/утроить данные средства, а после переводов денежных средств перестает выходить на связь.

Справочно: за 2022 год зафиксирован 1 факт указанной категории. 10.08.2022 житель Каменецкого р-на в мессенджере Telegram связался со злоумышленником, представленным как профессиональный игрок на бирже (трейдер). После переводов денежных средств на счет трейдера, последний изначально убеждал заявителя в успехе совместного предприятия, однако к моменту выплат мнимых выйгрышей перестал выходить на связь. Общая сумма похищенных средств составила 1100 рублей.

4. ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ ОТ ХИЩЕНИЙ СРЕДСТВ В СЕТИ «ИНТЕРНЕТ»

Для того чтобы обезопасить себя и свои денежные средства от подобных способов хищения, необходимо:

1) не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW- коды, данные касательно последних платежей и срока действия пластиковых карт третьим лицам;

2) в ходе использования карты подключить и использовать технологию «3D Secure». На настоящий момент это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. Позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель банковской карты подтверждает каждую операцию по своей

карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон;

3) исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, каким бы то ни было способом;

4) вводить секретные данные только на сайтах, защищенных сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://;

5) производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

6) не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации);

7) подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2 – 4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга;

8) не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется компьютер общего доступа;

9) в ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

10) вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адресу. Это действие обеспечит максимальный уровень безопасности.

11) исключить перевод денежных средств, в том числе в качестве предоплаты, до момента получения заказываемого товара/услуги.

Помните, Ваша безопасность в Ваших руках!