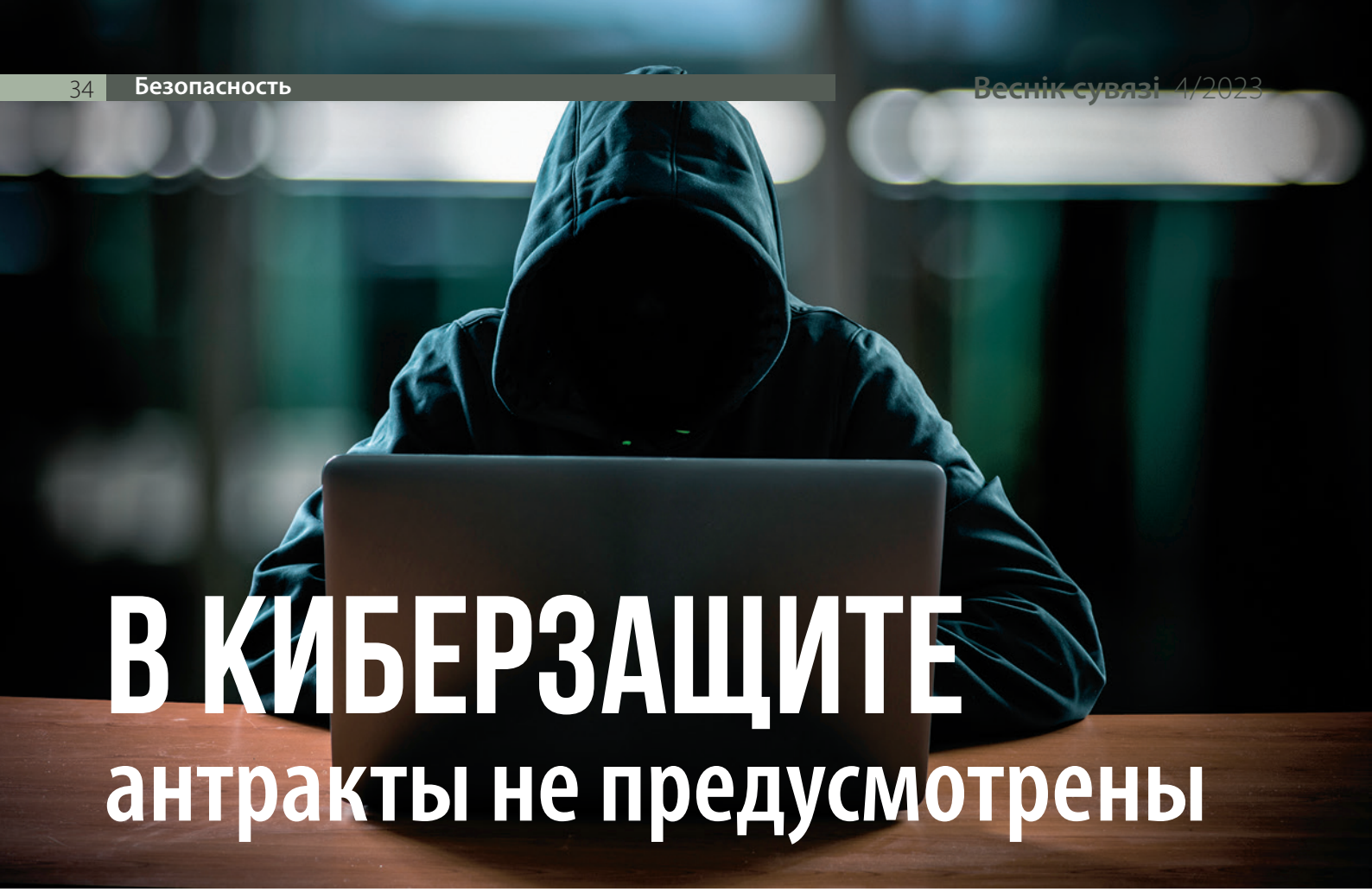

В КИБЕРЗАЩИТЕ антракты не предусмотрены

Давайте подумаем, что такое кибербезопасность? Это, наверное, то, что мы с вами не видим в повседневной жизни, но в любой момент можем с этим столкнуться, когда почувствуем ту или иную информационную угрозу. Например, наши персональные данные утекли в Сеть, кто-то снял деньги с нашей банковской карточки. Каждый может в любой момент столкнуться с киберугрозами…

На государственном уровне осуществляется многослойная структура защиты, которая четко определяет требования по кибербезопасности объектов информационной инфраструктуры. А что позволяет нам в таких случаях спать спокойно? Этим с редакцией «ВС» поделились эксперты в сфере кибербезопасности белорусского представительства известной компании «Лаборатория Kaspersky».

– Наиболее предметно ловушки злоумышленников активизировались в период летних отпусков, – говорит старший контент-аналитик **Ольга Свистунова**. – Специалисты выделили три основных вектора онлайн-мошенничества в этом направлении. Возьмем мошенничество с билетами. Эксперты видят множество поддельных страниц, имитирующих сайты разных авиакомпаний и агрегаторов по подбору авиабилетов. Некоторые из них даже могут отображать реальные данные о рейсах, отправляя поисковые запросы легитимным агрегаторам и выдавая полученную информацию. Однако настоящих билетов посетители фальшивых ресурсов не увидят. Цель злоумышленников – украсть деньги и использовать чужие личные данные в своих целях, например, чтобы продать их в даркнете.

Важный этап планирования поездки – поиск жилья, поэтому один из распространенных способов мошенничества – поддельные предложения об аренде квартир и апартаментов через интернет. Мошенники создают привлекательные объявления на популярных платформах, заманивая путешественников красивыми фотографиями и низкими ценами. Однако после бронирования и осуществления платежа окажется, что авторы объявлений вовсе не те, за кого себя выдают.

Еще один вид мошенничества с жильем связан с бронированием гостиниц. Мошенники создают поддельные сайты, имитирующие настоящие платформы бронирования отелей. Часто на таких сайтах пользователям предлагается войти в систему с учетными данными уже имеющихся аккаунтов. Это позволяет мошенникам получить несанкционированный доступ к учетным записям жертв в социальных сетях или электронной почте. Таким образом они крадут личные данные.

– Распространена афера с опросами, когда мошенники соз-

дают скам-страницы или рассылают электронные письма, в которых предлагают пройти опрос на тему путешествий и получить вознаграждение. В таких схемах расчет делается на желание людей получить легкие деньги или какой-либо подарок. Но нацелены они на сбор личных данных – имени, фамилии, адреса, номера телефона, финансовых сведений. Вознаграждение жертвы этой схемы не получают, а информация, которой они поделились с мошенниками, может быть использована, например, для кражи личных данных или денег. Кроме того, в конце опроса обычно предлагается поделиться информацией об опросе с друзьями, чтобы и они могли получить приз, то есть злоумышленники используют жертв еще и для дальнейшего распространения мошеннических ресурсов.

Поэтому мы напоминаем о необходимости проявлять осторожность при планировании поездок. Проверяйте подлинность сайтов, пользуйтесь надежными платформами бронирования и никогда не сообщайте личную или финансовую информацию без надлежащей проверки, – комментирует Ольга Свистунова.

«Это сотрудник банка» – так однажды могут обратиться по телефону, и эта фраза невольно вызывает внутреннее напряжение. Дальнейший диалог способен стать очередной популярной легендой злоумышленников.

По результатам исследования* Kaspersky в Беларуси, подавляющее большинство респондентов (70 %) сталкивались с телефонными и онлайн-мошенниками, которые представлялись сотрудниками финансовых организаций. Четверть участников отметила, что собеседники притворялись продавцами с сайтов с объявлениями, еще в 20 % случаев связывались якобы представители магазинов, а в 19 % – организаторы конкурсов или опросов.

По словам представителя Kaspersky в Беларуси **Дмитрия Кудревича**, самой распространенной легендой у мошенников является сообщение о подозрительных финансовых махинациях с картой или счетом (71 %). На втором месте располагается оповещение о выигрыше в лотерее или конкурсе и предложение его получить (46 %). Третье место занимает легенда о случайном переводе средств, а также последующая просьба их вернуть (21 %). Помимо этого, мошенники могут предложить поучаствовать в схеме с легким заработком (17 %) или сообщить о несчастном случае с родственником или знакомым (19 %).

В зависимости от легенды мошенники могут просить потенциальную жертву сообщить персональные или банковские данные (47 %), оплатить комиссию для получения выигрыша (34 %), назвать код из СМС или информацию с карты (33 %). Делать этого ни в коем случае нельзя.

– Чтобы обезопасить себя и не попасться на подобные уловки, – говорит Дмитрий Кудревич, – важно сочетать технические и нетехнические меры защиты: установить специальное решение, сохранять бдительность и повышать цифровую грамотность.

– Важно понимать, что злоумышленники специально маскируются под крупные и известные бренды: банки, интернет-магазины, сайты. Так они могут войти в доверие к жертве, и в итоге человек сам сообщает те данные, которые никогда никому нельзя передавать, – комментирует **Виктория Сацута**, представитель Kufar. – Чтобы не потерять деньги, важно придерживаться ряда простых правил:

- если вам звонят якобы из банка или магазина, положите трубку и перезвоните сами по официальным телефонам;
- не кликайте по ссылкам, которые вам присылают в мессенджерах. Не сканируйте QR-коды, которые к вам поступают;
- проверяйте адрес сайта, на котором находитесь. Мошенники отлично копируют дизайны, и отличить, где подделка, а где оригинал можно только по адресу в поисковой строке. Отличие даже в одном символе – признак того, что вы оказались на фальшивом сайте;
- никому не передавайте данные вашего паспорта, карты, коды из СМС;

- покупайте и продавайте только на официальных ресурсах, не переходите в сторонние мессенджеры, чтобы обсудить сделку.

В Беларуси с расширением информационно-коммуникационного поля выросло количество атак на Telegram. Мошенники обновили популярную схему кражи аккаунтов в мессенджере. Во втором квартале в Беларуси количество фишинговых атак на мессенджер выросло в 5 раз.

Специалисты компании отмечают, что количество попыток перехода белорусских пользователей на фишинговые ресурсы, мимикрирующие под Telegram, после непродолжительного спада, который начался в феврале 2023 года, вновь начало резко расти.

Начинается реализация схемы с того, что пользователя Telegram добавляют в канал. В нем злоумышленники размещают сообщения от имени некой женщины. Якобы у ее друзей дочь попала в финал конкурса рисунков, и нужно проголосовать за нее, чтобы девочка смогла выиграть путевку в лагерь. Для этого нужно набрать 500 голосов.

Фишинговое сообщение выглядит правдоподобно. Автор даже предлагает связаться с ней в личных сообщениях, если возникнут вопросы. В профиле размещена фотография человека, а не картинка. Чтобы проголосовать в конкурсе, нужно перейти по ссылке, которая также указана в сообщении. Однако в реальности человек попадает не на страницу с голосованием, а на фишинговый ресурс, который мимикрирует под страницу авторизации в Telegram. На нем человека просят ввести номер телефона и код подтверждения – именно эти данные и нужны злоумышленникам для кражи аккаунта.

– Telegram – популярный во всем мире мессенджер, чем не могли не воспользоваться атакующие. Если в первом квартале 2023 года количество попыток перехода белорусских пользователей по фишинговым ресурсам из Telegram исчислялось сотнями, то к концу второго квартала мы говорим уже о тысячах таких попыток. При этом злоумышленники постоянно адаптируют свои легенды и тактики под актуальную повестку, и обнаруженный фишинг это только подтверждает. Однако чем больше пользователи знают о различных видах угроз и схемах обмана, тем меньше у них шансов попасться на удочку интернет-мошенников, – комментирует Дмитрий Кудревич, представитель Kaspersky в Беларуси.

** Опрос проведен компанией OnIn по заказу Kaspersky в декабре 2022 – январе 2023 г. В Беларуси в нем приняли участие 505 человек из разных городов, в том числе Минска, Могилева, Гомеля, Витебска, Гродно, Бреста и др.*