**15 апреля 2022 года состоялась третья лекция из цикла тематических лекций, организованного АНО «ЦТЭД» в рамках проекта «Цифровая экономика для гражданского общества». Она была посвящена основным правилам кибербезопасности.**



«Как и запланировано, мы продолжаем наши тематические лекции. Сегодняшняя лекция, как и предыдущая, будет посвящена кибербезопасности, поскольку эта тема является особенно востребованной и актуальной для всех пользователей цифровых технологий. Перед нашими слушателями с практическими рекомендациями выступит уже знакомый им опытный эксперт по информационной безопасности, представитель Администрации Липецкой области Михаил Наумович Шахнюк», –сказала, открывая мероприятие, руководитель проекта «Цифровая экономика для гражданского общества» Наталья Маслова.

«Моя очередная лекция будет посвящена таким злободневным темам как мошенничество с использованием мобильных устройств и социальная инженерия, то есть разнообразныеманипулятивные психологические техники, которые используют преступники. Почему эти темы выделены в особую лекцию? Во-первых, у большинства пользователей основные денежные средства уходят как раз через мобильные устройства. И, во-вторых, социальная инженерия является той основой, с помощью которой совершаются мошенничества. К сожалению, в 99% случаев все наши проблемы связаны с тем, что мы не соблюдаем элементарные правила личной безопасности», – сказал Михаил Шахнюк.

«Сегодня самая большая ценность, которая у вас есть, это не кошелек и не банковская карточка. Это мобильный телефон. Именно он является основным средством идентификации и аутентификации. Это означает, что к телефону привязано практически все. Это и восстановление пароля на сайтах, и доступ к электронной почте имобильным кошелькам. Те же одноразовые пароли для совершения платежей – все идет через мобильник. Так как основная цель мошенников –получение прибыли, то именно телефон является их главной мишенью», – подчеркнул эксперт.

Михаил Шахнюк подробно рассказал о том, как происходит перехват SMS, о фальшивых точках доступа к WiFi, и особо остановился на человеческом факторе. Так, забытая SIM-картаможет стать инструментом доступа к личным средствам держателя банковской карты.

«Есть такие прецеденты, когда человек меняетномер телефона и через некоторое время у негоначинают уходить деньги с банковской карты. Поэтому, когда меняете номер телефона, не забывайте проверить все SMS-банкинги и вообще любые приложения, привязанные к этому номеру», – пояснил Михаил Шахнюк.

Михаил Шахнюк акцентировал внимание на том, что фактически безопасность каждого пользователязависит от одной-единственной SMS. «Если вы потеряли телефон и банковскую карту, то мошеннику вообще ничего делать не надо: достаточно знать номер карты и получить SMS на ваш телефон. Правило тут самое простое: получаете у сотового оператора SIM-карту и тут же устанавливаете на нее пароль!».

Как и на предыдущей лекции, все примеры лектор разбирал на сервисах Сбербанка. Он подчеркнул, что в мобильном приложении Сбербанка достаточно большой функционал по безопасности, который позволяет снизить риски и обеспечить надлежащий уровень безопасности. Так, в разделе «Настройки» имеется пункт «Лимиты и ограничения». Можно ограничить размер разового снятия наличных в банкомате и ограничить видимость банковских карт, то есть сделать так, чтобы карта не была видна в банкомате или на мобильных устройствах. Еще одна функция – это запрет покупок в Интернете без подтверждения SMS.

«Вы можете помочь не только себе, но и своим близким, особенно людям пожилого возраста. В «Сбербанк Онлайн» предусмотрена такая услуга, как проверка банковской операции близкого человека. Суть состоит в том, чтобы все операции вашего родственника, которые он хочет осуществить через мобильное приложение, будут приходить к вам на подтверждение», – сообщил эксперт.

Далее Михаил Шахнюк перешел к анализу манипулятивных тактик кибермошенников. В этом смысле они мало отличаются от обычных аферистов: они используют одни и те же методы социальной инженерии для получения доступа к конфиденциальной информации. «Разница лишь в том, что кибермошенники для своих афер применяют и информационные технологии» – заметил эксперт.

Он отметил, что с началом пандемии COVID-19, когда многим людям вынужденно пришлось перейти к работе в режиме онлайн, заметно участились случаю цифрового мошенничества, в том числе на Портале госуслуг, а также случаи мошенничества с недвижимостью, кредитами и SIM-картами.

Лектор дал целый ряд практических рекомендаций, указав, что для безопасности следует всегда использовать двухступенчатый вход с обязательным подтверждением через СМС. Целесообразно запретить регистрацию любых действий со своей недвижимостью без своего личного присутствия. Также необходимо регулярно проверять свою кредитную историю и то, какие электронные подписи созданы на ваше имя (это можно сделать в разделе «Настройки и безопасность» Портала госуслуг). Он подробноразъяснил, каковы правила использования электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Также Михаил Шахнюк рассказал о некоторых классических мошеннических схемах, например, что делать, если к вам на карту неожиданно поступили деньги от неизвестного человека.

В заключение он остановился на опасностях, связанных с излишне подробным освещением событий собственной жизни в социальных сетях. «Мошенники черпают информацию о человеке,изучая личные страницы социальных сетей, и действуют соответственно».

По окончании мероприятия слушатели через чат поблагодарили лектора за доступное изложение материала и практическую ориентированность его рекомендаций.

Лекция проводилась для слушателей, которыеприступили к изучению блока 3 «Основы кибербезопасности» Учебно-методического пособия «Цифровая экономика для гражданского общества» в рамках полного курса обучения продолжительностью 26 часов. Лекция в [записи](file:///C%3A%5CUsers%5C%D0%BB%D0%B5%D0%BD%D0%BE%D0%B2%D0%BE%5CDocuments%5Chttps%3A%5Cus06web.zoom.us%5Crec%5Cshare%5CEcFxcbJE3W6rHb0Q2AUcWFYgjuPE4wIBAjsCh-VKzeRbARjoseoK1bNfCeoXTQZl.JXzEv4UbBIFP3XEp)доступна всем остальным участникам проекта.

Лекция прошла в режиме видеоконференции. Всего было организовано 42 точки подключения, которыми воспользовались более 50 человек из Лангепаса, Мегиона, Нижневартовска, Урая, Югорска, Ханты-Мансийска, поселков Березовского и Советского районов, а также из Липецкой области.

Напомним, что по проекту «Цифровая экономика для гражданского общества» в рамках второго этапа проходят обучение 35 групп слушателей (350 человек) из шести муниципальных образований Югры: Лангепаса, Мегиона, Урая, Югорска, Ханты-Мансийска, Березовского, Советского и Нижневартовского районов. Также обучение по проекту проходит в Липецкой области.

Проект осуществляется АНО «Центр технологий электронной демократии» в тесном взаимодействии с Общественной палатой Югры при поддержке Департамента информационных технологий и цифрового развития и Департамента образования и науки ХМАО-Югры.

Технологическое обеспечение тематической лекции осуществлял МИП «ИНТЕХ» при Нижневартовском государственном университете на платформе Zoom.

Проект «Цифровая экономика для гражданского общества» реализуется на грант губернатора Югры.