**2 ноября прошла вторая лекция из цикла тематических лекций, организованного «Центром технологий электронной демократии» в рамках проекта «Цифровая экономика для гражданского общества». Она была посвящена основным правилам кибербезопасности.**

Лекция прошла в режиме видеоконференции. АНО «ЦТЭД» были организованы 62 точки подключения, которыми воспользовались около 80 человек из Лангепаса, Мегиона, Урая, Югорска, поселков Березовского и Советского районов, а также из Липецкой области.

Лектором выступил эксперт по информационной безопасности, представитель Администрации Липецкой области Михаил Шахнюк.

Он посвятил свое выступление теме мошенничества с использованием мобильных устройств и социальной инженерии как одной из главных современных киберугроз. Михаил Наумович пояснил, что социальной инженерией называют методы, которыми пользуются мошенники, чтобы «взломать» людей с целью незаконно получить от них ценную информацию или средства доступа к ней.

«Самым уязвимым звеном в технологической цепочке по-прежнему остается человек. Он имеет прямой доступ к информации и на него можно воздействовать методами социальной инженерии. Мошенникам зачастую вообще не требуется разбираться в технологиях – им достаточно использовать психологические манипуляции и социологические знания» – подчеркнул Михаил Шахнюк.

«В наше время самое важное и ценное, что находится в вашем кармане, это не кошелек – это телефон или планшет. Точнее, это SIM-карта, на которую завязаны все права доступа, включая восстановление паролей, «привязку» к сайтам и электронной почте», – продолжил он, и настоятельно рекомендовал в случае потери телефона, первым делом и как можно скорее заблокировать SIM-карту.

Не следует забывать и о той опасности, которую несут мобильным устройствам вредоносные, т.н. «вирусные» программы. Эксперт проиллюстрировал свою мысль конкретными примерами.

Например, мошенники могут использовать программу, которая, попав на устройство, перехватывает SMS-сообщения, включая сообщения от банков с динамическим паролем. В результате она от имени держателя карты начинает делать небольшие переводы (с лимитом до 8 000 рублей). Михаил Шахнюк посоветовал слушателям поставить на все свои мобильные устройства антивирусную программу.

«Надо учитывать, что SIM-карта мобильного телефона может сама по себе стать опасным элементом доступа к личным средствам держателя банковской карты. Дело в том, что при расторжении договора, неактивности карты и т.д. через 3-6 месяцев оператор сотовой связи отдает номер другому клиенту. Тому начинают приходить SMS-сообщения по чужой карте, а злоумышленники пользуются этим для хищения средств с карты настоящего держателя» - добавил Михаил Шахнюк.

Михаил Шахнюк снова вернулся к уже рассмотренной в ходе первой лекции цикла теме фальшивых точек доступа Wi Fi, которые используются мошенниками для перехвата персональных данных. Он рекомендовал в общественных местах вводить персональные данные, логин и пароль для оплаты банковских счетов или другую чувствительную и конфиденциальную информацию только через точки доступа, в которых пользователь уверен, или через сеть 3G.

Эксперт также рассказал о защитных функциях «Сбербанк-онлайн», включая настройки безопасности, блокировку банковской карты, услуги мобильного банка и отключение опции «Быстрый платеж», и остановился на основных видах электронной подписи и принципах их использования согласно Федеральному закону «Об электронной подписи» от 06 апреля 2011 года N 63-ФЗ.

По окончании лекции Михаил Наумович ответил на вопросы слушателей, дал ряд конкретных рекомендаций и вновь призвал пользователей мобильных устройств к бдительности.

**Справка:**

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

Лекция проводилась для слушателей, которые приступили к изучению блока 3 «Основы кибербезопасности» Учебно-методического пособия «Цифровая экономика для гражданского общества». Лекция и презентация будут доступны всех участников проекта.

Напомним, что по проекту «Цифровая экономика для гражданского общества» проходят обучение 35 групп слушателей (350 человек) из шести муниципалитетов автономного округа (Лангепаса, Мегиона, Урая, Югорска, Березовского и Советского районов и Липецкой области).

Проект разработан и реализуется АНО «Центр технологий электронной демократии» в тесном взаимодействии с Общественной палатой Югры при поддержке Департамента информационных технологий и цифрового развития и Департамента образования и молодежной политики.

Проект реализуется за счет гранта губернатора Югры.

