3 ноября прошла третья тематическая лекция по основным правилам кибербезопасности в рамках проекта «Цифровая трансформация на службе граждан», организованная АНО «ЦТЭД»

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

В режиме видеоконференцсвязи к лекции подключились тьюторы и слушатели из городов: Ханты-Мансийск, Нягань, Покачи, Радужный, а также из пяти поселений Кондинского района.

Всего было организовано 53 точки подключения, которые использовали около 130 человек, включая группы слушателей из образовательных организаций.

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

Как отметила исполнительный директор ЦТЭД Наталья Маслова, лекции Михаила Шахнюка отличаются высоким уровнем, что и обуславливает их востребованность у слушателей проекта.

«Мы сотрудничаем с Михаилом Наумовичем уже не первый год, и каждый раз получаем только самые позитивные отзывы о его лекциях. Запрос на достоверную и качественную информацию о том, как защититься от мошенничества в интернете, постоянно усиливается. Это вполне объяснимо: цифровые средства коммуникации вошли в повседневную жизнь и способствовали улучшению ее качества. Но, как это обычно и бывает, вместе с новыми возможностями появились и новые риски. Мы надеемся, что лекции Михаила Шахнюка помогут нашим слушателям не только освоить эти навыки самим, но и поделиться ими с друзьями и знакомыми» - сказала Наталья Маслова.

Михаил Шахнюк начал свое выступления с того, что 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, то есть то, что сейчас называется социальной инженерией» – сказал Михаил Шахнюк.

Он особо подчеркнул, что между кибер- и обычными мошенниками нет принципиальной разницы - они используют одинаковые манипулятивные тактики, разница лишь в том, что кибермошенники для своих афер применяют еще и цифровые технологии. Он привел несколько характерных примеров. Так, преступники создают сайты-клоны популярных инвестиционных компаний и убеждают доверчивых пользователей открыть личный кабинет и перевести через него средства «брокеру». Затем на карту жертвы мошенничества приходит относительно небольшая сумма – 10 или 15 тысяч рублей. Поверив в легкий заработок, некоторые пользователи впадают в ажиотаж, начинают переводить лжеброкеру сумму за суммой и даже берут

с этой целью кредиты. Оценив, что больше от пользователя ничего не получить, мошенники бесследно исчезают.

Далее эксперт перешел к рекомендациям. Он обратил внимание слушателей на то, что, как правило, все права доступа, включая восстановление паролей, «привязку» к сайтам и электронной почте, бывают завязаны на одну-единственную SIM-карту сотового телефона и настоятельно рекомендовал в случае потери телефона, первым делом и как можно скорее ее заблокировать.

Михаил Шахнюк также дал ряд ценных практических советов:

– С максимальной осторожностью относиться к сообщениям, полученным от незнакомых людей и к странным, не похожим на обычные сообщения от знакомых из списка контактов.

– Обязательно обращать внимание на расширения загружаемых файлов.

– Никогда не устанавливать на телефон никакие приложения из непроверенных источников и не давать им дополнительных прав в системе.

– Вводить личные/персональные данные только в проверенных местах, чтобы не столкнуться с фальшивыми точками доступа Wi Fi, которые используются мошенниками для перехвата персональных данных..

– В обязательном порядке установить на телефон антивирусную программу.

– Регулярно проверять доступ к своим учетным данным (почте).

– Также регулярно проверять, какие номера телефонов подключены к банковским услугам и кредитным картам.

Михаил Шахнюк особо остановился на защитных функциях сервиса «Сбербанк-онлайн», включая настройки безопасности, блокировку банковской карты, услуги мобильного банка и отключение опции «Быстрый платеж». Также он рассказал, какие меры по защите от кибермошенничества предусмотрены на Портале государственных и муниципальных услуг РФ.

В заключение Михаил Шахнюк рассмотрел основные виды электронных подписей и принципы их использования согласно Федеральному закону «Об электронной подписи» от 06 апреля 2011 года N 63-ФЗ.

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

Напомним, что по проекту «Цифровая трансформация на службе граждан» проходят обучение на первом этапе 25 групп слушателей (не менее 250 человек) из муниципальных образований Югры: г.г. Ханты-Мансийск, Нягань, Покачи, Радужный, а также из пяти поселений Кондинского района.

Справка:

Проект «Цифровая трансформация на службе граждан» направлен на обучение граждан цифровым компетенциям, необходимым для жизни в современном обществе.

Проект организует АНО «Центр технологий электронной демократии» при поддержке Департамента информационных технологий и цифрового развития и Департамента образования и науки Югры. Методическую и консультационную поддержку учебного курса осуществляет Малое инновационное предприятие «Интеллектуальные технологии» при Нижневартовском государственном университете, имеющее образовательную лицензию.

Проект реализуется за счет средств гранта губернатора Югры.