

## **14 апреля состоялась вторая тематическая лекция по основным правилам кибербезопасности в рамках проекта «Цифровая трансформация на службе граждан».**

Лекция была посвящена основным правилам кибербезопасности и борьбе с финансовым мошенничеством. Лекция проводилась для слушателей, которые приступили к изучению блока 3 «Основы кибербезопасности» Учебно-методического пособия «Цифровая трансформация на службе граждан» в рамках полного курса обучения продолжительностью 30 часов. Она прошла в режиме видеоконференции. Всего было организовано 22 точки подключения на образовательной платформе «Сферум».

Открывая лекцию, руководитель проекта «Цифровая трансформация на службе граждан», исполнительный директор АНО ЦТЭД Наталья Маслова, поблагодарила Департамент образования и науки Ханты-Мансийского автономного округа-Югры за поддержку и содействие в проведении тематических лекций для слушателей проекта.

В этот раз к лекции присоединилось 55 слушателей из Ханты-Мансийска, Нягани, Радужного, Покачей, а также из Кондинского района. Они использовали возможность подключиться к лекции лично или из компьютерных классов. Несколько групп слушателей еще изучают материалы блока 1 - «Основы цифровой грамотности» и блока 2 – «Ресурсы и сервисы цифровой экономики» Учебного плана курса «Цифровая трансформация на службе граждан», поэтому лекция для них будет доступна в записи.

«Цифровая трансформация создает условия для решения многих проблем, но вместе с новыми возможностями появляются и новые угрозы. Мы надеемся, что лекции Михаила Шахнюка помогут нашим слушателям противодействовать этим угрозам, а также поделиться информацией с родными и друзьями», - сказала Наталья Маслова.

Лектор начал свое выступление 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.

Далее лектор отметил: «SIM-карта мобильного телефона становится опасным элементом доступа к личным средствам держателя банковской карты. При расторжении договора, неактивности карты и т.д. через 3-6 месяцев оператор сотовой связи отдает номер другому клиенту, которому начинают приходить СМС-сообщения по чужой карте. Злоумышленники пользуются этим для хищения средств с карты настоящего держателя». Михаил Наумович также дал ряд ценных практических советов: с максимальной осторожностью необходимо относиться к сообщениям,

полученным от незнакомых людей и к странным, не похожим на обычные сообщения от знакомых из списка контактов; никогда не устанавливать на телефон никакие приложения из непроверенных источников и не давать им дополнительных прав в системе; регулярно проверять, какие номера телефонов подключены к банковским услугам и кредитным картам; 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 устанавливать антивирусные программы и т.п.

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.

Лектор рассмотрел основные виды электронных подписей и принципы их использования согласно Федеральному закону «Об электронной подписи» от 06 апреля 2011 года № 63-ФЗ. Он подчеркнул: «Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью».

Особо отметил Михаил Шахнюк то, 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 технологии. Он привел примеры, как преступники создают сайты-клоны настоящих инвестиционных компаний для торговли на бирже. Затем они убеждают россиян зарегистрироваться в личном кабинете и перевести средства якобы на брокерский счет. И на карту жертвы потом приходит сумма в 10-15 тыс. рублей. Поверив в легкий заработок, многие впадают в эйфорию и переводят лжеброкеру гораздо большие суммы, в том числе взятые в кредит, после чего мошенники исчезают.

В заключении эксперт рассказал о новейших видах киберугроз, связанных с внедрением систем искусственного интеллекта и нейросетей. В современном цифровом мире киберугрозы постоянно развиваются. Широкое использование искусственного интеллекта в кибератаках стало одним из самых значимых событий последних лет. По мере развития технологий ИИ злоумышленники используют их для проведения более изощренных и эффективных атак. Например, такое новое явление — дипфейки (deepfake), поддельный контент с наложением лиц и голосов известных людей на видеоматериалы различного содержания с применением технологий искусственного интеллекта.

Завершил свое выступление Михаил Наумович тем, что предупредил: «Наверно, многие уже знают, что ChatGPT — это большая языковая модель и веб-приложение на её основе, созданные компанией OpenAI. Как только ChatGPT появилась, люди начали думать, в каких практических областях мы

можем её применить. И злоумышленники здесь — не исключение. Они тоже изучают, как ChatGPT можно использовать для киберпреступлений. Это серьезная опасность завтрашнего дня».

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 Ханты-Мансийского автономного округа-Югры и Департамента образования и науки Ханты-Мансийского автономного округа-Югры.

Методическую и консультационную поддержку учебного курса осуществляет Малое инновационное предприятие «Интеллектуальные технологии» (МИП «ИНТЕХ») при Нижневарттовском государственном университете, имеющее образовательную лицензию.

Проект реализуется за счет средств гранта губернатора Югры.

