

"От технологий не убежать"

Борис КОСТИШКО принял участие в проекте «Вопрос ректору».

Проект Российского союза ректоров дает возможность руководителям университетов высказаться на актуальные темы. Комментарий Бориса Костишко был посвящен итогам работы цифровых кафедр в вузах.

— 2022/2023 учебный год помимо прочего был отмечен массовым открытием в университетах цифровых кафедр, где дают базовые знания по IT-направлению, в том числе непрофильным студентам. Насколько успешным это начинание оказалось для вашего вуза? Где вы нашли преподавателей, учебные программы? Каким оказался спрос со стороны студентов?

— Начнем с того, что убежать от информационных технологий в современном обществе в принципе невозможно. Поэтому в той или иной степени все должны уметь ими пользоваться. Я намеренно использовал слово "должны", потому что эти навыки напрямую определяют качество жизни человека. И здесь нет абсолютно никакой

разницы, какая у вас профессия, физик вы или лирик. Теперь эти навыки не удел избранных.

Так что обучение непрофильных студентов совершенно точно не мода, а жизненная необходимость. В прошлом году по программе "Цифровые кафедры" в УлГУ обучалось 639 человек, а в 2023 — уже 1 084 студента.

Вопрос о преподавателях всегда самый актуальный, но в нашем университете 12 направлений подготовки "цифровых" студентов и, соответственно, есть свои высококвалифицированные преподаватели. Кроме того, для составления учебных программ и организации образовательного процесса мы привлекаем партнеров — ведущие IT-компании: SimbirSoft, ZeBrains, Simtech Development и Cart-Power.

Первый блин однозначно не оказался комом. Студенты достаточно ответственно отнеслись к учебе, это и понятно — они понимают необходимость "цифровых"



знаний. Показательно и то, что все прошли промежуточную оценку знаний и продемонстрировали улучшение своих компетенций.

Хочу выразить надежду, что цифровые кафедры в университетах станут постоянно действующими и обучение в них будут проходить абсолютно все студенты.

Безопасность

ЗАЩИТИТЬ СВОЁ

Участились случаи телефонного мошенничества в отношении сотрудников учебных заведений.



В России зафиксировали рекордное число попыток телефонного мошенничества. Показатель достиг 9 миллионов звонков сутки. Злоумышленники придумывают все новые схемы, попасться на удочку может самый бдительный.

90 % всех случаев кибермошенничества приходится на телефонное. Самой популярной остается схема с переводом или взносом на "безопасный счет". Сбербанк оценил, что к такому типу относится 77 % всех попыток мошенничества. Распространенными уловками этой схемы являются звонок от якобы службы безопасности банка о смене финансового номера, оформление кредита на клиента и попытка снять у него деньги.

В последнее время мошенники стали чаще отправлять россиянам в соцсетях поддельные документы, в том числе из банка. При этом злоумышленники активно обзванивают целые семьи. Они представляют себя сотрудниками банка или полиции, сообщают о возможном похищении денежных средств и просят принять меры. Членов семьи стремятся убедить в реальности угрозы и просят повлиять на своего родственника.

Основой мошеннических схем служит персональная информация, полученная на нелегальном рынке баз данных интернет-магазинов, финансовых учреждений, государственных структур. Усложнив методы своей работы, киберпреступники могут долго обрабатывать очередную жертву, чтобы убедить ее перевести деньги, соблазняя финансовой выгодой и даже предлагая некую должность с высокой оплатой. Ради этого устраивают видеособеседования с потенциальным "работодателем".

Весьма распространена схема воровства "на доверии". Так, телефон из объявления в интернете или СМИ о продаже любого имущества немедленно попадает в поле зрения мошенников. И владельцу звонит некий "потенциальный покупатель", готовый платить, не торгуясь, но только на карту. Для этого он просит сообщить ее номер, срок действия, CVV-код.

Участились случаи телефонного мошенничества в отношении сотрудников учебных заведений. В случае получения сообщения в мессенджере (WhatsApp, Viber, Telegram и т.д.) от имени ректора, проректора с просьбой позвонить сотруднику Министерства науки и высшего образования для решения каких-либо финансовых и иных вопросов, необходимо незамедлительно перезвонить в приемную руководителя вуза для подтверждения полученной информации.

Еще один вид мошенничества направлен на получение доступа к личному кабинету на портале госуслуг. Не переходите по ссылкам в письмах от "Госуслуг" с информацией, которую вы не запрашивали. Все сообщения от портала дублируются в личном кабинете. Проверьте там наличие сообщения, пришедшего на почту. Будьте внимательны к адресу отправителя — письма от "Госуслуг" приходят только с одного адреса — po-reply@gosuslugi.ru. Официальные рассылки от "Госуслуг" никогда не содержат призывов оставить СНИЛС или банковские реквизиты, они носят общий информационный характер.

Как проверить номер, с которого поступают звонки? В интернете существует достаточно много сервисов для того, чтобы определить если не владельца конкретного телефонного номера, то по крайней мере город или страну, откуда пришел звонок. До 40 % таких сообщений производятся из-за границы, еще 40 % — из мест заключения. В любом случае поможет звонок в проверенную службу безопасности или колл-центр банка, а не по указанному грабителем номеру.

Главная примета мошенников — навязчивый инструктаж. Помните, что на самом деле сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают другими способами. Получив звонок от незнакомого человека, обратите внимание на то, что и как он хочет вам сообщить. Мошенники стремятся теми или иными способами надавить на жертв — торопить, запутывать, угрожать возможными последствиями. В такой ситуации важно сохранять спокойствие. Даже если вам угрожают потерей всех денег на счетах, не спешите выполнять требования звонящего.

Мошенник может несколько раз подряд задавать жертве вопросы, на которые можно ответить только словом "да". Столкнувшись с такими вопросами, старайтесь давать другие ответы, переспрашивать или переводить тему.

Если вам звонят из банка — попробуйте задать уточняющие вопросы, например, о состоянии счета или последних операциях по карте. Скорее всего, злоумышленник ничего не сможет ответить. Если вам предлагают какую-либо выплату — уточните основание, на котором она производится.

Мошенники стремятся получить секретные данные карты, настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства.

Если вы столкнулись с телефонным мошенничеством — как можно скорее обратитесь в полицию, даже если вы не отправляли деньги или данные карты. В заявлении подробно опишите обстоятельства происшествия — время звонка номер телефона, ФИО и "должность" звонящего, содержание и итог разговора, если вы переводили деньги — отправленную сумму. В качестве основания укажите статью 159 УК РФ (если мошенник смог получить от вас деньги) и часть 3 статьи 30 УК РФ (если этого сделать не удалось). Если у вас есть запись звонка (его можно записать с помощью специального приложения) — приложите ее к заявлению.

Пётр ИВАНОВ.

Наука

АТОМ В ПОМОЩЬ

Ученые УлГУ начали испытания лекарства для сверхточного уничтожения рака.

Специалисты российской атомной отрасли начали доклинические испытания радиофармацевтического препарата для "прицельного" уничтожения рака предстательной железы. Масштабы распространения онкологических заболеваний требуют применения новых радиоактивных изотопов для их лечения. Такими изотопами признаны так называемые альфа-излучатели, эффективно убивающие раковые клетки и позволяющие значительно повысить выживаемость пациентов по сравнению с традиционной химиотерапией.

Ученые приступили к доклиническим исследованиям таргетного радиофармпрепарата на основе изотопа тория-227 и антител, предназначенного для лечения рака предстательной железы. Исследования будут проводить специалисты всерегионального объединения "Изотоп", входящего в "Росатом", на базе Научно-исследовательского технологического института имени С.П. Капицы Ульяновского государственного университета. Работа над проектом рассчитана до середины следующего года. Он реализуется в кооперации с ведущими научными центрами России — Российским научным центром радиологии и хирургических технологий имени академика Гранова, Научно-исследовательским институтом атомных реакторов, Институтом элементоорганических соединений РАН и инновационной частной компанией "Инова плюс", ведущей молекулярно-биологические исследования.



Торий-227 будет использоваться в комплексе с антителами, связанными с белком — простат-специфическим мембранным антигеном. Этот белок содержится в здоровых клетках предстательной железы, но при раке его уровень существенно увеличивается. Уже получен так называемый биоконъюгат путем соединения наноантитела с торием-227. В ходе доклинических исследований будет проверена безопасность готовой лекарственной формы для пациентов и ее эффективность по отношению к опухолевым клеткам, после чего начнутся клинические исследования радиофармпрепарата.

Ника БОРИСОВА.