СЛУЖБА БЕЗОПАСНОСТИ УНИВЕРСИТЕТА ОБРАЩАЕТ ВАШЕ ВНИМАНИЕ НА УЧАСТИВШИЕСЯ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ.

Существуют следующие методы информационно-психологического воздействия:

- мошенничество с банковскими картами (телефонное мошенничество);
- телефонный терроризм, угрозы и запугивание родственников Российских военнослужащих;
- враждебные, ненавистнические комментарии под выступлениями известных личностей, призывы к насилию;
- информационные вбросы, раскручивание историй с известными людьми, призывы к выступлениям;
- давление искусством слова и фактами;
- использование эмоций людей, направление на неосознанные и поспешные действия;
- идеологические и информационные провокации, диверсии с целью давления на мировое сообщество в соцсетях, иностранных СМИ;
- подходы невоенного воздействия;

- организация митингов и протестов;
- влияние на общественно-политические настроения, поиск уязвимостей;
- вбросы выгодной, зачастую недостоверной информации;
- использование рекламного сервиса для распространения пропаганды;
- хакерские атаки на различные ресурсы России и других стран;
- многочисленные ложные сообщения о готовящихся терактах.

Цели информационно-психологического воздействия:

- давление на мировое сообщество;
- разжигание межнациональной розни, создание паники;
- влияние на общественно-политические настроения в своих целях;
- организация беспорядков, волнений;
- создание негативного имиджа России и дружественных стран;
- пропаганда русофобии;
- дискредитация Вооруженных сил РФ;
- манипулирование сознанием граждан;
- формирование нужного представления о ком-либо и о чем-либо в интересах противников России;
- продвижение идеи смены режима, вражды;
- создание негативной ситуации, паники.

Противостояние информационно-психологическому воздействию:

- полное игнорирование;
- не вступать в полемику;
- не отвечать на комментарии;
- знать, что каждый несет личную ответственность за распространение ложной информации, при этом не имеет значение, что его обманули;
- осознанный подход к применению информации;
- должна быть адекватная реакция и осознанное восприятие реальности;
- не дать себя обмануть;
- ориентироваться в потоке информации;
- смотреть на информационный поток как на атаку и отражать её;
- не быть зависимым от информационных вбросов, а рассматривать все аспекты, проблемы, составляющие событий и информации;

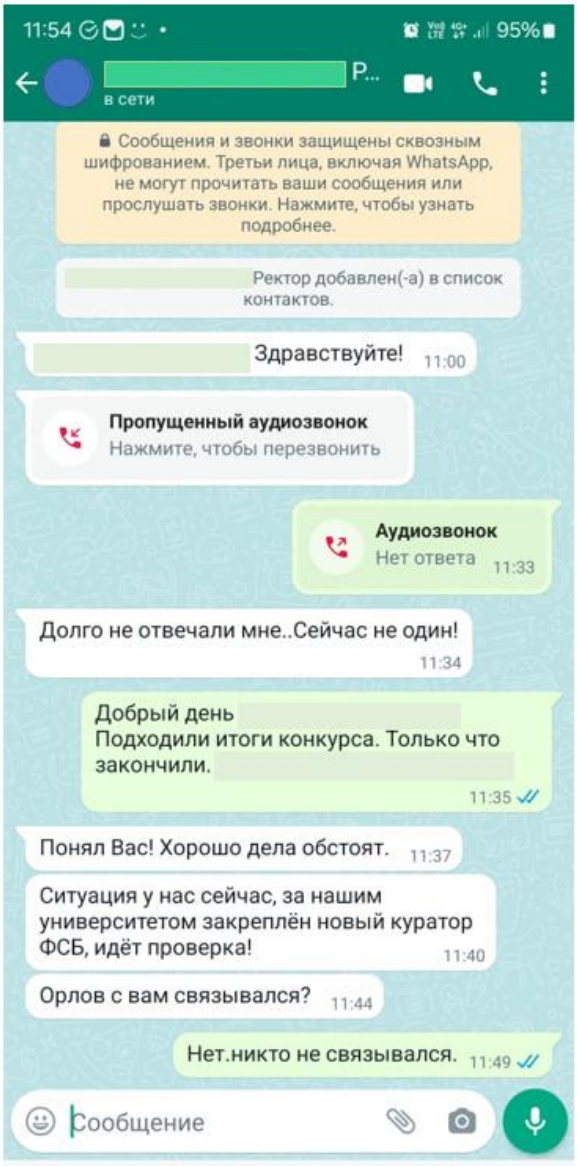
- ориентироваться в нормативных актах РФ, регламентирующих ответственность за распространение дискредитирующей информации.

Продолжаются попытки хищения путем обмана денежных средств у преподавателей.

Мошенники представляются сотрудниками исполнительных органов власти, силовых структур, ссылаются на высокие должности. В целях осуществления своих мошеннических действий злоумышленники используют различные технологии подмены голоса и используют для связи, в том числе, такие мессенджеры как Telegram, WhatsApp и Viber.

В мессенджерах мошенники легко могут поставить себе аватарку (фотографию известного вам человека, картинку или иное графическое изображение) с логотипом Сбербанка, Госуслуг, правоохранительных органов, чтобы вызвать ваше доверие.

Все чаще используется следующая схема: сначала звонок якобы от Ректора Университета: «С Вами свяжется сотрудник ФСБ, окажите всевозможное содействие»; затем звонок якобы от сотрудника ФСБ: «Все должно остаться в тайне»! По итогу все заканчивается тем, что необходимо



заплатить серьезную денежную сумму или выполнить какие-либо противоправные действия!

«Лжесотрудники убеждают граждан в том, что как только они перечислят денежные средства, выявить мошенников станет проще, так как при снятии денежных средств со счетов их данные становятся видны сотрудникам правоохранительных органов». В разговоре мошенники обещают вернуть деньги после завершения «спецоперации».

Злоумышленники пытаются не только выманить деньги у своих жертв, но и ввести в заблуждение правоохранительные органы и навредить российским гражданам — звонки по большей части поступают из кол-центров недружественных стран.

На сегодняшний день подмена номера — один из наиболее распространенных способов телефонного мошенничества. Эксперты по кибербезопасности отметили, что при использовании метода подмены номеров с помощью IP-телефонии можно позвонить от лица любого абонента. Злоумышленники используют его, чтобы ввести граждан в заблуждение, а также затруднить работу правоохранительных органов по установлению злоумышленника.

Злоумышленники могут позвонить от имени банка, силовых структур и т.д., при этом у потенциальной жертвы высветится именно тот номер, что был задан злоумышленниками.

Для подмены мошенники используют реальные номера полиции, банков, госучреждений или номера абонентов физлиц.

Участились случаи звонков, когда серьезный голос представляется чином из ФСБ и пугает, что с вашей карты были совершены денежные

переводы в поддержку украинских военных. Даже если вы не знали об этом, вы все равно являетесь изменником родины и вам светит очень серьезный срок с конфискацией всего имущества. Особенно пугаются таких звонков пожилые люди, сутками сидящие у экранов телевизоров, на них и рассчитаны звонки. Мошенники предлагают перевести деньги на «безопасные» счета.

Помимо отъема денежных средств мошенники могут убедить жертву совершить противоправные действия: например, поджечь банкомат или отделение банка и даже совершить нападение на военкомат. Это не собственно схема мошенничества, но один из видов воздействия на пострадавших: преступники убеждают их в том, что именно в банке или в военкомате находятся настоящие преступники – бросив туда бутылку с зажигательной смесью, жертва поможет «выкурить» из здания обманщиков, которых тут же арестуют правоохранители. Но в действительности уголовное дело заводится на жертву.

Пользователям можно посоветовать прежде всего скептически относиться к внезапным звонкам от людей, которые представляются сотрудниками банков, государственных учреждений и так далее. Нужно помнить, что ни при каких обстоятельствах сотрудники организаций не будут просить вас сообщить данные банковской карты, учетной записи в онлайн-банке или другом сервисе, а также одноразовые пароли, которые приходят по SMS или в push-уведомлениях. **Никогда не устанавливайте по просьбе неизвестных людей ПО на свои устройства**.

К сожалению, есть эпизоды, когда мошенникам удается достигнуть желаемого результата и получить деньги обманным путем.

В связи с этим, всем руководителям структурных подразделений необходимо провести инструктаж работников и обучающихся о рисках телефонного мошенничества. Именно сейчас в сфере образования ведется усиленная подрывная деятельность со стороны вражеского центра информационно-психологических операций (ЦИПсО)!

НАПОМИНАЕМ ОБЯЗАТЕЛЬНЫЕ ДЛЯ ВСЕХ ПРАВИЛА ПОВЕДЕНИЯ!

1. В случае поступления звонков, якобы от руководства, необходимо доложить своему непосредственному руководителю о поступившем звонке. В

последующем, непосредственному руководителю необходимо уточнить достоверность поступившего звонка у вышестоящего руководства.

2. В случае поступления любых ссылок в переписке или при разговоре на сотрудников правоохранительных органов, необходимо доложить в Службу безопасности Университета или заместителю руководителя по безопасности.

3. Если суть разговора или поступивших сообщений сводится к тому, что необходимо перечислить какие-либо денежные средства или выполнить какие-либо противоправные действия, необходимо **НЕЗАМЕДЛИТЕЛЬНО** проинформировать свое руководство и обратиться в правоохранительные органы!

4. Когда вам звонят от имени полиции или Пенсионного фонда, банка или налоговой, военкомата или страховой компании, не верьте на слово. Сразу кладите трубку, если от вас требуется перевести куда-то деньги или назвать, к примеру, номер карты и код из SMS.

ЧТО ДЕЛАТЬ, ЕСЛИ ПОСТУПАЮТ СООБЩЕНИЯ ОТ ЗЛОУМЫШЛЕННИКОВ?

Имеются случаи, когда недоброжелатели, выдавая себя за руководство Университета, рассылают письма с требованием предоставить личные данные. В свете этих событий, мы хотим напомнить вам о важности защиты вашей личной информации и предлагаем следующие рекомендации:

1. **Относитесь критически к внезапным запросам.** Официальные органы обычно не обращаются к отдельным работникам от имени руководства организации с запросами о предоставлении личных данных.

2. **Проверяйте источник сообщения.** Если вы получили письмо, которое кажется подозрительным, обратите внимание на электронный адрес отправителя. Недоброжелатели могут использовать адреса, которые похожи на официальные, но имеют незначительные отличия или полностью маскироваться под отправителя.

3. **Не передавайте личную информацию.** Никогда не предоставляйте личные данные, такие как номер телефона или банковские данные, в ответ на подозрительные письма. Если у вас возникли сомнения, свяжитесь с отправителем письма другим способом или обратитесь в департамент информационных технологий для проверки письма.

4. **Сообщайте о подозрительной активности.** Если вы получили подозрительное письмо, не отвечайте на него и немедленно сообщите об этом в Департамент информационных технологий.

5. **Берегите свою репутацию.** Недоброжелатели могут использовать страх перед нанесением вреда репутации как способ манипуляции. Помните, что защита ваших личных данных — это также защита репутации Университета.

БУДЬТЕ БДИТЕЛЬНЫ, ВНИМАТЕЛЬНЫ И ОСТОРОЖНЫ!

Наша общая безопасность и защита информации — это наша общая ответственность.

При поступлении сомнительных телефонных звонков и сообщений, а также по фактам информационно-психологического воздействия обращаться непосредственно в Службу безопасности Университета (Москва, Миусская пл.. д. 9, каб. № 192, ул. Героев панфиловцев домовл. 20, каб. № 325), телефон: 8(499) 978-99-60, 8 (499) 250-17-89 или по электронной почте: sbrhtu@muctr.ru