COVID-19: актуальные угрозы безопасности конфиденциальной информации

На сегодняшний день отмечается значительный рост уровня угроз безопасности конфиденциальной информации, в том числе содержащей персональные данные, связанных с использованием нарушителями неблагоприятной эпидемиологической ситуации с коронавирусной инфекцией COVID-19 – эпидемия внесла коррективы в мировую экономику и в жизнь обычных людей, ситуация отразилась и на информационной безопасности. По некоторым данным[1], широкое применение цифровых технологий в повседневной жизни привело к росту киберинцидентов в I квартале 2020 года на **22,5 %**, по сравнению с IV кварталом 2019 года, причем объектами атак выступали преимущественно государственные учреждения, промышленные предприятия, медицинские организации. Мотивами злоумышленников в **34 %** случаев была кража персональных данных граждан, 19 % - данные платежных карт и в 15 % случаев учетные данные (логин и пароль).

Сложившаяся ситуация требует от каждого из нас новых навыков, позволяющих защитить себя, свои персональные данные, имущество, денежные средства и многое другое в цифровой среде. Ставропольским государственным медицинским университетом совместно с Управлением Роскомнадзора по СКФО был выработан ряд рекомендаций по данной проблеме, направленных на широкую аудиторию, прежде всего наших абитуриентов, обучающихся, пациентов и работников:

1. Публикуйте как можно меньше информации о себе и личных данных в социальных сетях. Не секрет, что каждая социальная сеть – бесценный, и, порой неисчерпаемый источник информации для злоумышленников, собирающих персональные данные, которые используются для обмана и мошенничества.
2. Не публикуйте онлайн фотографии документов, билетов, платежных чеков – это самый простой способ узнать о том, когда и как долго вас не будет дома.
3. Не используйте открытые Wi-Fi-сети. Они могут выглядеть как вполне надежный источник Интернета, предоставленный местным кафе или даже библиотекой, но вам будет сложно отличить «добропорядочный» Wi-Fi от «зловредного». Чтобы создать такую сеть, преступнику понадобятся всего лишь ноутбук и Wi-Fi-адаптер. Мошенники используют этот метод, чтобы перехватить логины и пароли пользователей, пытающихся подключиться к Интернету с помощью их Wi-Fi-сетей.
4. Используйте стойкий пароль. Слабые комбинации практически ни от чего не защищают, злоумышленник сможет относительно быстро узнать вашу секретную комбинацию знаков методом подбора. Регулярно обновляйте свой пароль – не менее одного раза за полгода.
5. Защищайте свою электронную почту. Как правило, ваша почта хранит «ключи» от большинства ваших учетных записей, так как процедура восстановления пароля чаще всего осуществляется именно с помощью email-сообщений.
6. Не открывайте электронные сообщения, полученные от сомнительного источника. Злоумышленники быстро подхватили тему всеобщего беспокойства по поводу коронавирусной инфекции и стали использовать ее для фишинговых писем. Около 13 %

[1] Национальный координационный центр по компьютерным инцидентам, компания Positive Technologies

атак, в которых киберпреступники задействовали методы социальной инженерии, были связаны с коронавирусом. В 78% атак на медицинские учреждения были задействованы методы социальной инженерии. Злоумышленники рассылали сотрудникам фишинговые письма, цель которых — убедить получателя ввести корпоративные учетные данные в поддельную форму аутентификации

7. Установите антивирусную защиту на всех электронных устройствах, следите за обновлением антивирусных баз.

8. Проверяйте подлинность сайта, на котором планируете ввести свои учетные данные. Например, популярный ресурс для предоставления государственных и муниципальных услуг – Госуслуги (www.gosuslugi.ru) имеет множество поддельных доменных имен, созданных злоумышленниками. Проверяйте безопасность соединения с сайтом (наличие цифрового сертификата), большинство популярных интернет обозревателей сообщают о неблагонадежности ресурса.

Дополнительную информацию вы можете получить в отделе организации и технологии защиты информации управления по стратегическому развитию по телефону +7 (8652) 75-41-10.