Уважаемые коллеги !

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупреждает об активном использовании злоумышленниками ситуации вокруг пандемии коронавируса COVID-19 для осуществления широкого спектра вредоносной деятельности и публикует рекомендации по противодействию угрозам компьютерной безопасности, связанным с его распространением (https://safe-surf.ru/specialists/news/645362/).

Специалисты НКЦКИ выделяют два типа вероятных угроз: Мошенничество и угрозы, связанные с удаленным режимом работы.

Рекомендации по противодействию угрозам компьютерной безопасности :

1. Проявляйте осторожность при обработке электронных сообщений с темой, вложением или гиперссылкой, связанных с COVID-19. Не раскрывайте личную или финансовую информацию в электронном письме и не отвечайте на запросы о предоставлении этой информации.
2. Используйте официальные источники для получения актуальной, основанной на фактах, информации о COVID-19.
3. Для предотвращения кражи персональных данных подключайтесь только к проверенным интернет-платформам для проведения видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, мобильных приложений для доставки еды и т.д.
4. Прежде чем делать пожертвования, проверяйте подлинность благотворительных организаций во избежание кражи денежных средств.

Рекомендации по обеспечению информационной безопасности при удаленном режиме работы

1. Убедитесь, что средства антивирусной защиты на выданном Вам служебном компьютере (ноутбук) надлежащим образом настроены и функционируют.
2. Проверьте сервис, который используется для удаленного доступа к ЕМТС (если ViPNet Client установлен на Ваш личный ноутбук).
3. Используйте удаленный доступ в ЕМТС строго с двухфакторной авторизацией (сначала вводите учетное имя и пароль ViPNet Client и только после установления защищенного соединения учетное имя и пароль пользователя ЕМТС) и ни кому не разглашайте/передавайте указанную идентификационную информацию.

4. Организуйте контроль за подключением внешних устройств, в том числе USB-носителей информации, к устройству, предназначенному для удаленного доступа в ЕМТС.

5. Проверьте, что электронная почта защищена двухфакторной авторизацией (не используйте сервисы типа «сохранить пароль»). Необходимо обеспечить анализ электронной почты антивирусными средствами.

6. Используйте стойкий пароль к управляющей панели домашнего роутера и WPA2 шифрование при подключении к сети Интернет с применением Wi-Fi (проверьте, изменен ли заводской пароль к управлению домашним роутером на Ваш личный).

7. Акцентируйте внимание на фишинговых атаках, связанных с тематикой COVID-19.

8. Установите ограничение доступа к удаленному рабочему месту детей, родственников и посторонних лиц, а в случае невозможности – установите ограничения прав их учетных записей.

Памятка по соблюдению несложных правил цифровой гигиены в связи с мероприятиями, направленными на предупреждение распространения новой короновирусной инфекции

Специалисты Департамента информационных технологий города Москвы проанализировали основные обманные сценарии и подготовили инструкцию для горожан, как избежать фишинга –кражи личных данных.

Эксперты по информационной безопасности относят фишинг к самой популярной форме интернет-мошенничеств. Его главная цель – получение доступа к конфиденциальным сведениям. К ним относятся персональные данные, служебные записи, пароли от платежных систем и банковских карт. Для получения необходимых материалов мошенникам нужно, чтобы человек прошел по ложной ссылке и оставил на сайте-подделке личную информацию. Для побуждения к действиям преступники используют разные уловки – от обещаний невероятного дохода до угроз и запугиваний. Сейчас преступники спекулируют на страхах, связанных с пандемией коронавируса, используя разные сценарии. Эксперты ДИТ Москвы собрали основные из них.

Письмо из ООН. Москвичи получают на электронную почту письма якобы от имени официальных международных организаций и государственных органов - ВОЗ, ООН, МВФ и даже МКС.

В сообщениях содержатся общеизвестная информация о мерах безопасности или статистике заболеваний и прилагается ссылка на фишинговый сайт. При переходе на него человеку предлагают ввести свои персональные данные. Именно здесь и происходит их хищение или заражение вредоносными программами пользовательских устройств - смартфонов, компьютеров, планшетов.

Кампании по сбору денег. От этих же международных отправителей горожанам приходят письма-призывы присоединиться к мировым акциям по сбору средств для заболевших, эвакуации наших граждан их зарубежных стран, разработки вакцины против вируса и даже для спасения мировой экономики. Мошенники предлагают перечислить символические суммы, но гораздо большую ценность для них представляют введенные на сайте-«близнеце» данные для доступа к платежным системам и банковским картам.

Продажа «дефицитных» товаров. Пользуясь ажиотажным спросом, мошенники предлагают купить москвичам медикаменты, средства профилактики и гигиены, рекомендованные для защиты от коронавируса. Среди лидеров продаж – индивидуальные маски, антисептики, перчатки. Когда пользователь пытается оформить покупку, мошенники крадут банковские данные.

Тест на коронавирус. Тесты на определение коронавируса или вакцина от него – это фейковое предложение уже для состоятельных пользователей. Цена несуществующих экспресс-полосок на выявление инфекции COVID-19 достигает 15 000 рублей, а эффективной вакцины, как известно, еще не разработано ни в одной стране мира. Для любителей эзотерики рассылают объявления по продаже магических средств защиты: амулетов, оберегов, заговоренных браслетов. Их стоимость еще выше – до 300 тысяч рублей. Кроме денег, потраченных впустую, впечатлительный пользователь после интернет-покупки лишится и других сбережений, как только мошенники получат доступ к банковской карте.

Звонки из «больниц». Кроме e-mail-рассылок фишинг-преступники используют телефонные сообщения и звонки. Они поступают от имени лже-врачей инфекционных отделений, сотрудников Роспотребнадзора и других больниц и ведомств. Взволнованным родственникам сообщают, что их близкие госпитализированы и изолированы с диагнозом коронавирус, а затем предлагают перевести деньги на фальшивый счет «медучреждения» для улучшения условий содержания больного и его лечения. Финал аналогичен другим сценариям: вымогательство денег и кража личных данных.

Уведомления от туроператоров. Письма от имени туроператоров, транспортных организаций, страховых компаний о возврате денежных средств за путевки, билеты, страховые полисы — еще одна актуальная сейчас схема выманивания персональных сведений у граждан. Пользователю предложат заполнить какое-либо заявление с указанием необходимых данных.

Удаленная работа. С переходом на удаленную работу участились случаи рассылки писем от корпоративной техподдержки, банков, госорганов с уведомлением о смене режима и предложением воспользоваться ссылками для дистанционного подключения к служебным ресурсам. Преступники получают учетные данные пользователей и атакуют в дальнейшем информационные системы организаций.

Сценарии у преступников разные, но цель всегда одна – хищение личных данных. При этом есть и официальные полезные рассылки, информирующие или предупреждающие горожан о важных изменениях. Жители получают своевременные предупреждения от оперативных служб, уведомления от коммунальных, подписываются на новости интересных им компаний. Поэтому не надо бояться всех рассылок или смс-сообщений без исключения. Главный совет - не спешите и будьте внимательны»

Для защиты личных данных и борьбы с фишингом достаточно выполнять несложные, но действенные рекомендации :

Обращать внимание на адрес отправителя. Проверять, существует ли данный адрес, указан ли он в качестве контактного на официальном сайте организации.

Не переходить по ссылкам в письме. При наведении курсора мышки на ссылку, в нижнем левом углу браузера будет отображен адрес сайта, на который хотят перевести. Если этот адрес сайта и ссылка в письме не идентичны, ссылка фишинговая, переходить по ней не стоит.

При переходе на сайт внимательно смотреть на внешний вид страницы. Поддельные ресурсы чаще всего повторяют интерфейс официальных.

Не вводить данные от учетных записей и банковскую информацию на сайтах, не поддерживающих функцию шифрования. Обязательно в адресной строке браузера должен быть отображен зеленый или закрытый замок, а перед ссылкой стоять такой набор символов: «https://».

Обращать внимание на мелочи, проверять информацию, даже если письмо пришло от знакомого вам человека, не скачивать вложения и пользоваться антивирусными программами на своих устройствах. При звонках с угрозами и вымогательством денег записать звонок, зафиксировать номер и обращаться в полицию.

При телефонных звонках из банка сразу положить трубку, позвонить в банк по номеру, указанному на банковской карте, и сообщить о попытке мошенничества. Можно также обратиться в правоохранительные органы. Сотрудник банка никогда не станет спрашивать номер банковской карты, CVV-код, пин-код, код из СМС, логин и пароль от онлайн-банка.

Официальные рассылки идут от одного имени с постоянным и одинаковым написанием. Например, MCHS. Обращать внимание на расширение после знака @ в почтовых рассылках. Оно повторяет корпоративное написание или доменное имя главного сайта (press_dit@mos.ru).

Не заходить в интернет-банк и на другие важные сайты через Wi-Fi в кафе, отелях, торговых центрах. Не подключаться к общедоступным сетям, где не требуется ввод пароля.

С особым вниманием относиться к сообщениям про коронавирус. Сейчас это тема №1 в мире, и мошенники ею пользуются. Узнавать информацию только из достоверных источников.