Методические рекомендации по информационной безопасности при работе с электронной почтой

В ходе мониторинга угроз информационной безопасности в сети Интернет, осуществляемого региональными центрами Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) наблюдается постоянный рост количества, усложнение и совершенствование мошеннических схем, использующих массовые рассылки подложных электронных писем.

Мошенники, используя почтовые домены, похожие на официальные адреса международных организаций, органов государственной власти Российской Федерации, пользуясь ажиотажем вокруг новостей о распространении коронавируса в мире, начали осуществлять рассылку вредоносного программного обеспечения под видом документов, якобы, содержащих статистические сведения о распространении коронавирусной инфекции или официальные рекомендации по борьбе с ней.

Зафиксированы факты ложных рассылок, исходящих, якобы, от Центров по контролю и профилактике заболеваний (Centers for Disease Control and Prevention), от Всемирной организации здравоохранения (World Health Organization, WHO), а также использующих темы коронавируса (CoViD-19, SARS-CoV2).

Как правило, письма, носящие вредоносный характер, имеют своей целью методами социальной инженерии склонить получателя к открытию вложенных файлов, либо к переходу по Интернет-ссылкам на сторонние ресурсы.

В случае, если получатель такого письма из любопытства осуществит указанные действия, то на его компьютер внедряется вредоносная программа. Это может быть программа-троян (скрытно осуществляющая поиск в компьютере и передачу хозяину секретных паролей, реквизитов банковских карт и персональных данных жертвы), рекламная закладка (захламляющая рабочий экран рекламными сообщениями), программа-майнер (тайно осуществляющая генерацию криптовалюты), а в худшем случае - вирус-шифровальщик, осуществляющий шифрование жесткого диска с последующим вымогательством денежных средств у своей жертвы. Следует помнить, что вирусная опасность со стороны электронной почты грозит в настоящее время не только стационарному компьютеру, но и мобильным гаджетам - смартфонам и планшетам.

В некоторых случаях при переходе на ложный (подконтрольный злоумышленникам) сетевой ресурс пользователь под различными предлогами (проверка мер безопасности, сбои в работе систем и т.п.) побуждается к введению своего логина и пароля доступа в систему (в личный кабинет).

Преступниками для достижения своих целей используются официальная символика и логотипы известных организаций и органов государственной власти, а также предпринимаются меры по визуальной маскировке адресов электронной почты с помощью замены одной или нескольких букв или

использования специальных символов (пример: tater.ru или talar.ru, вместо tatar.ru), а также изменение доменной зоны (пример: вместо tatar.ru - tatar.gov).

В некоторых случаях поддельное письмо можно выявить по наличию грубых орфографических или стилистических ошибок в тексте.

Для минимизации риска заражения служебных и личных компьютеров, а также мобильных гаджетов при приеме и обработке электронной почты настоятельно рекомендуется:

- проявлять бдительность и тщательно проверять любой факт поступления на Ваш электронный почтовый ящик информации, не относящейся к вашему основному виду деятельности, либо направленной Вам впервые;

-

- не отвечать на запросы от имени «технических», «сервисных» и тому подобных служб любых организаций с просьбой сообщить свои логины, пароли, личные данные, реквизиты банковских карт, номера документов, время своего отсутствия в квартире, любую другую информацию о себе и своей семье, перепроверять факт запроса путем телефонного звонка официальным представителям данной организации;

- не открывать вложения, полученные из неизвестных источников и не переходить по ссылкам, которые находятся в текстах таких писем, в том числе, направленных от лица, якобы, органов государственной власти, силовых и правоохранительных структур, проверять факт направления файла путем телефонного звонка. В случае невозможности установить происхождение письма, необходимо его **удалить, не сохраняя и не запуская** вложенные файлы;

- регулярно обновлять антивирусное приложение, операционную систему и веб-браузер, предпочитать лицензионные антивирусы бесплатным;

- осуществлять регулярное резервное копирование важной для Вас информации на внешние носители;

- никогда не отключать встроенные средства защиты операционной системы.