В настоящее время, на фоне осложнения эпидемиологической обстановки в мире, экспертами в сфере информационной безопасности прогнозируется рост числа рассылок вредоносного программного обеспечения, «фишинговых» писем, а кибератак на компьютеры, оборудование (роутеры, видеокамеры) и незащищенные домашние сети сотрудников организаций, которые перешли на удаленный режим работы. Целью кибератак станет хищение денежных средств или персональных данных пользователей.

С целью получения доступа к безналичным денежным средствам физических и юридических лиц, персональным данным, иной ценной информации, злоумышленники осуществляют фишинговые рассылки с использованием злободневных тем в том числе о якобы наличии вакцины от актуальных вирусных заболеваний, последних статистических данных или способах борьбы с болезнью. На самом же деле за рассылкой стоят злоумышленники, которые все более изощренными способами используют страхи и сумятицу.

Кроме того, для привлечения внимания потенциальных жертв злоумышленниками могут использоваться реквизиты различных международных благотворительных организаций, а также финансовых учреждений страны. Так, уже зафиксирована вредоносная рассылка с троянской программой внутри, при этом письма отправляются якобы от лица сотрудницы UNICEF — международной организации, действующей под эгидой ООН, а также под видом Всемирной организации здравоохранения. Зачастую к «фейковому» письму прилагался архив, который содержал «троян», совмещающий функционал программы для кражи логинов-паролей и клавиатурного шпиона. Например, он может собирать данные о системе и зараженном компьютере, загружать и запускать файлы, делать скриншоты, управлять клавиатурой и мышью, похищать логины, пароли, а также данные банковских карт.

Для того, чтобы обезопасить свои денежные средства и конфиденциальную информацию, на современном этапе лучше скептически относиться к любым поступающим сообщениям об актуальных вирусных заболеваниях — как об их распространении, так и о средствах защиты, доверяя только крупным надежным источникам, особую внимательность стоит проявлять, получая письмо, содержащее в себе ссылку и текст, призывающий по ней перейти. Чтобы избежать опасности, рекомендуется игнорировать все подобные сообщения и вместо этого заходить на официальный сайт соответствующих организаций или на их страницы в социальных сетях.

Организация безопасной работы в удаленном режиме также имеет свои особенности и требует соблюдения ряда дополнительных требований:

- на персональный компьютер, используемый для работы следует установить лицензионное антивирусное программное обеспечение и произвести его верные настройки, а при работе с электронной почтой следует дополнительно использовать антивирусное программное обеспечение, отвечающее за защиту почтовых сервисов и анализирующие поток данных, проходящий через них;
- при обработке входящей корреспонденции, поступающей по каналам электронной почты следует обращать внимание на прикрепленные к письмам файлы и не допускать их открытия (запуска) непосредственно из почтовой программы. Целесообразно сохранить вложение (не запуская его) и проверить его на наличие вредоносного программного обеспечения. Наличие у поступивших вложений двойного расширения или автоматическое его скрытие может свидетельствовать о прикреплении к файлу вредоносного программного обеспечения;
- USB-ключ с электронной цифровой подписью следует подключать к персональному компьютеру только непосредственно при проведении необходимых финансовых операций;
- заранее позаботьтесь о получении удаленного доступа к необходимым ресурсам и следуйте указаниям специалистов по информационной безопасности своего предприятия для его настройки;
- по возможности работайте на корпоративном компьютере. Постарайтесь не загружать и не открывать корпоративные файлы на личных устройствах;
- домашние сети не защищаются специалистами по информационной безопасности предприятия, поэтому будьте внимательны – атакующие могут воспользоваться ситуацией и направить усилия на менее защищенных пользователей;
- проверьте, настроена ли двухфакторная аутентификация в почте, в мессенджерах и при VPN подключении;
- обязательно смените стандартный пароль домашнего роутера, иначе злоумышленники легко смогут получить доступ к вашим данным;
- объясните близким, что Вашим рабочим компьютером пользоваться нельзя, чтобы избежать случайного заражения устройства или потери данных.