Мошенники пытаются заработать на COVID-19.
В интернете увеличилось количество фишинговых атак

В первом квартале 2020 года в Гродненской области по линии информационной безопасности отмечается снижение количества совершенных преступлений по сравнению с аналогичным периодом прошлого года на 20,5 %. Вместе с тем, пандемия коронавируса влияет и на Интернет-пространство. Злоумышленники всего мира активно используют широкое обсуждение в Интернете и в электронной переписке тематики COVID-19.

По информации компании «Barracuda Networks», обеспечивающей сетевую безопасность более 220000 глобальных корпоративных клиентов, начиная с февраля 2020 года количество связанных с коронавирусом фишинговых атак увеличилось на 66,7 %, достигнув более 9 000 атак только в марте этого года. В период с 1 по 23 марта 2020 года «Barracuda Networks» обнаружила 467 825 фишинговых атак электронной почты по всему миру, и 9 116 из них были связаны с COVID-19. **Для сравнения, в феврале 2020 года было выявлено в общей сложности 1188 связанных с коронавирусами фишинг-атак, а в январе 2020 года – только 137 атак.**

Анализ свидетельствует о том, что в ходе различных фишинговых кампаний используется фактор повышенного внимания к COVID-19 для распространения вредоносных программ, кражи учетных данных и выманивания денег у пользователей посредством мошеннических действий. В ходе таких атак реализуется обычная регулярно наблюдаемая фишинговая тактика. Вместе с тем, все большее число фишинговых атак использует коронавирус как приманку, чтобы попытаться обмануть находящихся в подавленном состоянии пользователей, извлекая выгоду из страха и неуверенности своих предполагаемых жертв.

Исследователи выделяют три основных типа фишинговых атак с использованием тематики коронавируса COVID-19: мошенничество, использование имитации бренда и компрометация деловой электронной почты.

Квалифицированные злоумышленники используют такие эмоции как смущение и страх, чтобы вызвать реакцию на свои попытки фишинга и тем самым обмануть людей и выудить у них деньги. Принимая во внимание наличие у людей страха и неуверенности, вызванных ситуацией с коронавирусом COVID-19, а также элемент сочувствия, злоумышленники нашли конкретные ключевые эмоции для использования.

К примеру, «Barracuda Networks» выявила атаку с использованием шантажа, в которой утверждалось о наличии доступа к личной информации о жертве, включая ее местонахождение, и высказывалась угроза заразить жертву и ее

семью коронавирусом в случае, если не будет выплачен выкуп.

Многие обнаруженные мошенники пытались продать лекарства от коронавируса или маски для лица, либо просили инвестировать средства в фиктивные компании, которые, якобы, разрабатывают вакцины от COVID-19.

Мошенничество в форме запросов на пожертвования для фальшивых благотворительных организаций с использованием фактора коронавируса – еще один популярный метод фишинга.

Помимо широко распространенного сбора учетных данных посредством вредоносных программ, фишинговые атаки со ссылками на поддельные страницы входа в систему также используют коронавирус COVID-19 в качестве приманки. Один из таких вариантов, например, декларирует себя в качестве составной части Агентства по контролю за заболеванием и пытается украсть учетные данные «Microsoft Exchange» при щелчке по вредоносной ссылке.

Злоумышленники также подделывают большое количество различных страниц входа в систему электронной почты, ориентируясь на порталы электронной почты, к которым привыкли пользователи. При этом злоумышленники взламывают информацию данного почтового сервера. Другие страницы входа являются более общими либо предлагают несколько вариантов для провайдера, подделывая страницу входа каждого провайдера. Злоумышленники просто изменяют существующую авторизацию для осуществления фишинга электронной почты, извлекая выгоду посредством использования фактора коронавируса.

Несмотря на то обстоятельство, что фишинговые письма использующие коронавирус, представляют собой новое явление, выработаны определенные рекомендации для обеспечения безопасности электронной почты. **Необходимо:**

- остерегаться любых электронных писем, пытающихся заставить пользователей открывать вложения или щелкать ссылки;
- следить за сообщениями, которые поступают от источников, от которых вы обычно не получаете электронные письма. Это вероятные попытки фишинга. Несмотря на то, что получение электронных писем, связанных с коронавирусом, в рамках списков рассылки, к которым вы принадлежите, становится обычным делом, следует тщательно проверять электронные письма от организаций, от которых вы не получаете регулярные сообщения;
- быть осторожными с электронными письмами от организаций, с которыми вы регулярно общаетесь. Это особенно актуально для тех, кто

работает в сфере здравоохранения, поскольку на эту сферу нацелены кибератаки, пытающиеся извлечь выгоду из стрессового давления, вызванного работой с возрастающим количеством инфицированных коронавирусом;

- осуществлять поиск заслуживающих доверия благотворительных организаций и делать пожертвования напрямую Обычная тактика мошенничества, связанного с коронавирусом заключается в запрашивании пожертвований в помощь пострадавшим от пандемии. Тем самым будет обеспечено попадание финансовых средств именно туда, где эти средства могут делать добро, а не в руки мошенников. Также весьма маловероятно, что какие-либо законные благотворительные организации принимают пожертвования через биткойн-кошельки, поэтому такие электронные письма должны однозначно настораживать.

В контексте пандемии COVID-19 некоторые веб-сайты предоставляют электронные формы для заполнения так называемой «Декларации о персональной ответственности», необходимой для осуществления дальнейших действий. Такие Декларации также могут быть попытками фишинга. В этом случае вредоносный URL достигает потенциальных жертв не по электронной почте, а через социальные сети. Данные, собранные соответствующими веб-сайтами, могут использоваться для различных целей, таких как выполнение хакерских действий от имени лица, заполнившего форму, или определение временных интервалов, когда человек не находится в своем доме, с целью организации кражи по этому адресу. В данном конкретном случае рекомендуется использовать Декларацию только с веб-сайтов государственных учреждений, которая может быть загружена, распечатана и заполнена вручную, без передачи личной информации через Интернет.