

Рекомендации по эффективному распознаванию фишинговых писем

Разъясняет помощник прокурора Промышленного района

Татаров Тамаз Тамазович

Что такое фишинговые письма?

Фишинг (англ. phishing) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель - вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Это позволяет ослабить концентрацию человека, усыпить его бдительность.

Так, применение различных психологических приемов делает такой вид интернет-мошенничества чрезвычайно эффективным.

Какие должны быть первоначальные действия при получении электронного письма?

Если Вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у Вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

ожидаю ли я это письмо?

есть ли смысл в том, что от меня требуют?

знаю ли я автора этого письма?

уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «нет» - внимательно проанализируйте содержимое письма.

Имейте в виду, что особого внимания требуют письма, которые: содержат ссылку для перехода на сторонний ресурс (возможно, ссылка ведет на фишинговый поддельный ресурс). При этом еще большего внимания заслуживают письма, содержащие «короткие ссылки», так как невозможно определить, куда ведет такая ссылка;

содержат вложение (возможно, файл содержит вредоносный код для заражения вашего компьютера);

составлены на иностранном языке;

имеют большое количество получателей;

содержат орфографические ошибки;

связаны с финансовой, банковской сферой или геополитической обстановкой.

Как анализировать электронные письма?

1. Проверьте адрес отправителя (домен адреса электронной почты, с которой пришло письмо, должен совпадать с доменом, указанным на официальном сайте организации, от имени которой якобы направлено письмо, а логин такой почты, в свою очередь, должен совпадать с принятой логикой их построения в той или иной организации). Проверяйте адрес отправителя, даже в случае совпадения имени с уже известным контактом;

2. Проверьте полное имя отправителя (для проверки полного имени отправителя, наведите курсор мышки на указанное в письме имя отправителя) и затем проанализируйте высветившийся адрес электронной почты в соответствии с информацией из официальных источников (см. пункт выше);

3. Проверьте, при наличии, ссылки, даже если письмо получено от другого пользователя Вашей почтовой системы, и помните о том, что сам факт направления Вам по электронной почте ссылок, ведущих на сторонний ресурс, является подозрительным:

- обратите внимание на название сайта, на который Вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (например, www.sObranie.ru). Кроме того, для введения в заблуждение злоумышленником могут быть использованы специализированные сервисы сокращения ссылок (например, bit.ly, tinyurl.com);

- наведите курсор мышки на ссылку (**не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна**) и проверьте, чтобы URL, указанный в электронном сообщении, и URL, отображаемый при наведении курсора на ссылку, совпадали;

- также Вы можете вручную (не копируя ее) вбить полученную ссылку в строке поисковой системы (yandex, mail.ru и др.). Такой метод позволит Вам заметить возможные «ошибки» в полученной ссылке;

4. Проверьте наличие вложений. Если отправитель, электронное письмо и причина, по которой Вас просят открыть вложение, вызывает даже самое незначительное подозрение - ни при каких обстоятельствах не открывайте его.

5. Обращайте внимание на возможные опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма;

6. Если полученное письмо вызывает сомнения, по возможности, свяжитесь с отправителем или со справочной организации, от которой пришло такое электронное письмо, по другому каналу связи. При этом контактные данные нужно брать из авторитетных источников, а не из направленного Вам письма.

Что делать, если Вы обнаружили фишинговое письмо?

1. Не переходите по ссылке, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок;
2. Не нажимайте на ссылки, если они заменены на слова;
3. Не копируйте адрес ссылки;
4. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
5. Не подгружайте картинки от незнакомых людей;
6. Не запускайте макросы в офисных приложениях (*макрос - это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи.*);
7. Не пересылайте письма коллегам, родным, близким и иным лицам;
8. Удалите фишинговое письмо.