Памятка по информационной безопасности

Основные правила защиты от фишинга

1. Проверяй адрес тех, кто Вам пишет

Если Вы получили сообщение от незнакомого отправителя, первое, на что стоит обратить внимание, — адрес отправителя.

Сверяйте домены всех отправителей подозрительных электронных писем с доменом, указанным на официальном сайте государственного учреждения или иной организации, которая ведёт с Вами «общение».
Мошенники обычно отправляют письма с общедоступных почтовых доменов — mail.ru, yandex.ru и т.п., или используют домены, похожие на официальные доменные имена компаний, *!!!!Иногда производится подмена домена почтового адреса, но создается имя несуществующего почтового ящика!!!!* чтобы ввести получателя письма в заблуждение.

2. Изучи письмо

Не спешите открывать ссылки в письме или скачивать вложенный файл, если:

- отправитель сообщения тебе не знаком
- в сообщении нет персонального обращения к Вам (фишинговые письма часто носят обезличенный характер, и обращение к получателю выглядит как «пользователь» или «клиент»)
- в электронном письме нет подписи отправителя, в переписке по электронной почте сотрудники любой организации оставляют подпись с указанием ФИО и

контактного номера телефона или адреса организации. Вы всегда можете связаться с человеком для проверки подлинности отправки, если альтернативный канал связи, кроме электронной почты, отсутствует – лучше перестраховаться.

- из текста письма не понятна суть — кто и по какой конкретной причине тебе пишет

3. Проверь ссылку

Подозрительная ссылка — один из основных признаков фишингового письма. Эти ссылки часто сокращаются мошенниками или форматируются так, что выглядят как ссылка, ведущая на официальный сайт, однако это не так. Проверяй любую ссылку, прежде чем ее открыть:

Способ 1

Наведи курсор мышки на ссылку в письме. В левом нижнем углу экрана браузера будет отображён адрес сайта, на который Вас хотят перевести

Способ 2

Нажми на ссылку правой кнопкой мыши, выбери «копировать гиперссылку». Открой любой текстовый редактор (Word, блокнот и т.д.) и вставь скопированный текст.

Если ссылка из Вашего письма и та, которую Вы увидите после проверки, будут отличаться, письмо прислали мошенники и открывать ссылку опасно. Помните, что фишинговые письма могут содержать веб-адрес, визуально похожий на настоящий адрес сайта, однако в ссылке может скрываться намеренная опечатка, например, «I» заменена на «1». Такая ссылка будет вести на фальшивый сайт, который создали мошенники.

4. Не скачивай вложения

Злоумышленники часто к своим сообщениям прикрепляют файл или добавляют ссылку, при нажатии на которую незаметно для пользователя, загрузится вредоносное программное обеспечение.

Вредоносное ПО может маскироваться под стандартную программу, которая будет работать в фоновом режиме и красть конфиденциальную информацию с устройства (данные банковских карт, учётные данные пользователя и многое другое).

Другой неблагоприятный сценарий — установится программа-вымогатель, которая зашифрует или удалит конфиденциальные данные с устройства жертвы в целях выкупа. Даже при оплате выкупа нет гарантий, что данные будут восстановлены.

Обращайте особое внимание на вложения с расширением exe, zip, rar, pdf – это наиболее часто используемые форматы электронного документа, содержащие в своем составе вредоносное ПО.

5. Будь внимателен к деталям

Плохая орфография, грамматика или пунктуация — это признаки фишингового письма.

За маской злоумышленников нередко встречаются малограмотные личности или те, кто вовсе не говорит на русском языке, а текст сообщения набирает с помощью онлайн-переводчика. Также в подписи письма мошенники могут указать придуманные имена, например, Мария Поппинс.

Обратите внимание и на детали письма, даты, места и другие нюансы, которые помогут понять, что данное письмо не имеет к Вам никакого отношения. Внимательность поможет не стать новой жертвой обмана.

6. Не торопитесь и взвесь ситуацию

Вас должно насторожить, если тема, контент письма или название файлов побуждают Вас к немедленному действию (к переходу по ссылке, к нажатию на кнопку, к открытию файла, к немедленному ответу на письмо), либо вызывают у Вас любопытство. Мошенники — хорошие психологи, и они используют любые способы, чтобы убедить жертву открыть ссылку или скачать вложение.