Многоликий фишинг (Часть 2)

В современной практике фишинга есть и более хитроумные способы обмана потенциальных жертв. Сегодня о некоторых из них.

Целая «гроздь» методов фишинга основана на подмене легального содержимого нелегальным – называется всё это «спуфингом». Фишеры наловчились умело подменять практически всё, что можно прислать в email-сообщении: отправителя и его email-адрес, тему письма, вложение в письмо, содержимое и ссылки на сайты. Например, email-адрес отправителя может выглядеть как вполне легальный, скажем, support@paypal.com. Нюанс здесь, однако, в том, что первая буква «а» в наименовании домена адреса (paypal.com) – кириллическая («русская»). Таким образом, подобный домен зарегистрирован злоумышленниками и не имеет никакого отношения к платёжному сервису PayPal. «На глаз» такая подмена неразличима.

Аналогичным образом поступают с доменами в ссылках фишинговых писем: такая ссылка может выглядеть почти как настоящая за счёт «мимикрии» – например, может вести на поддельный сайт mai1.ru вместо настоящего mail.ru. Иногда также используются похожие до смешения буквосочетания «rn» вместо «m» и «cl» вместо «d». Такую подмену заметить можно, но лишь присмотревшись.

Другой пример – динамическая подмена ссылки в email-сообщении: если навести «мышку» на ссылку в письме, будет отображён один адрес перехода, а при нажатии на ссылку специальный скрипт меняет ссылку, и в действительности пользователь переходит на поддельный сайт.

Именно поэтому лучший совет для борьбы с подменой ссылок и доменов – не полениться набрать ссылку самостоятельно в адресной строке браузера. Если у вас есть причины вообще открывать ссылку.

Иногда вы можете получить сообщение, в котором будет файл-вложение с именем, например, «rcs.mp3». Судя по расширению, резонно предположить, что вам прислали музыкальный файл в формате «mp3» (в которых крайне редко бывает какое-либо вредоносное ПО). На деле же, при открытии файла запускается троянская программа-вирус. Фокус в том, что если в имени файла поставить определённый невидимый так называемый управляющий символ, то имя файла меняется на обратное – то есть «3pm.scr» превращается в «rcs.mp3».

Ещё одним распространённым видом фишинга является направленный (целевой) фишинг – в этом случае фишинговая атака направлена не на неограниченно широкий круг неизвестных злоумышленнику жертв, а на вполне определённого, нужного для злоумышленника, человека. Целью является получение конфиденциальной информации конкретного пользователя-жертвы. Для этого злоумышленник предварительно осуществляет сбор информации о жертве. Если жертвой является высокопоставленное лицо, то подготовка целевой атаки может осуществляться очень тщательно, с применением всех законных и незаконных способов, при этом используются соцсети, сотовые операторы, базы госорганов и т.д. В итоге злоумышленник, хорошо зная фактическую информацию о «жертве», её круг общения, составляет сообщение, которое неминуемо должно вызвать доверие у «жертвы» и привести к совершению ею нужных преступнику действий по раскрытию своей конфиденциальной информации.

Такие атаки весьма трудоёмки и затратны, поскольку подготовка отнимает большую часть времени. Однако, усилия должны окупиться, поэтому целью подобных атак являются, как правило, не «простые люди». Как следствие, целевые атаки характеризуются намного более высокой эффективностью нежели обычный фишинг.

Ранее мы упоминали, что никакое ПО не может обеспечить 100% защиту от вредоносных сообщений, поэтому главным и наиболее действенным способом защиты от фишинга, в том числе, от целевого, является внимательность при использовании электронной почты и своевременный вопрос «зачем?» - «зачем я получил это письмо?». И если вы не можете ответить на этот вопрос, не ожидали такого письма и не знаете его отправителя – в 99% случаев такое письмо окажется спамом или фишингом (или и тем и другим).