Многоликий фишинг (Часть 1)

Фишинг – давно (если это слово применимо к связанным с интернетом вещам) известная совокупность методов несанкционированного получения киберзлоумышленниками конфиденциальной информации пользователей. Давно известная, но, тем не менее, совсем не потерявшая свою актуальность угроза – ежегодно миллионы пользователей по всему миру становятся жертвами изобретательности фишеров, придумывающих всё новые разновидности фишинга.

Только ежедневно в мире рассылается около 3 с лишним миллиарда фишинговых писем. При этом, в 2021 году Россия оказалась на втором месте в мире по количеству пользователей, атакованных фишингом (6,33%, на первом месте – Испания с 9,32%). Кроме того, около 80% пользователей не в состоянии распознать фишинговые письма.

Почему фишинг выгоден злоумышленникам? Приличный «улов» (фишинг переводится с английского как «рыбалка») при вполне позволительных затратах. Арифметика фишинга примерно такова:

- Отправлено писем – 2 000 000 шт;
- Получено пользователями писем – 100 000 шт. (или 5%, большая часть всё же задерживается спам-фильтрами сетевого оборудования и почтовых серверов);
- Нажали на фишинговую ссылку – 5 000 чел (или 5%);
- Ввели данные на фишинговом сайте – 100 чел (или 2%);
- Средняя прибыль с каждой жертвы – 1200 долларов (согласно общемировой статистике);
- Итого общая прибыль лишь от одной фишинговой рассылки – 120 000 долларов.

Вполне неплохо, если учесть, что исходная рассылка выполняется автоматически и занимает меньше часа. Воистину, плохой день на рыбалке лучше, чем хороший день на работе!

Мы неоднократно писали, что фантазия злоумышленников практически неисчерпаема. Разнообразие методов фишинга – ещё одно тому подтверждение. Изобретательность преступников, позволяющая им с помощью самых хитроумных методов создавать практически неотличимые от реальных фишинговые письма или сайты, побуждая пользователя самостоятельно отдавать конфиденциальную информацию (или доступ к ней), у некоторых специалистов-безопасников вызывает даже нечто схожее с восхищением «красотой» реализации фишинга.

Наиболее часто используемым методом фишинга, конечно же, является email-фишинг или фишинг с помощью сообщений электронной почты. Обычно, ничего не подозревающий пользователь получает в свой почтовый ящик сообщение, в котором некто, обычно от лица какой-либо организации, просит пользователя выполнить некие действия – проверить правильность документа (а для этого открыть вложение в присланном сообщении), или подтвердить данные своей учётной записи, например, в онлайн-банке (а для этого открыть содержащуюся в письме ссылку, ведущую на умело мимикрирующийся под настоящий сайт с формой ввода данных, откуда они попадают прямо к злоумышленникам), или, наоборот, опровергнуть кем-то когда-то поданную на пользователя жалобу (иск, оформленный кредит, выставленный счёт и т.д.). Часто подобный призыв к действиям сопровождается словами «срочно» или «незамедлительно», или же получателю ставится определённый срок («если Вы не опровергните жалобу до 29 февраля, Вам отключат газ»), до которого он непременно должен выполнить требуемые жуликами действия. Таким образом злоумышленники вводят пользователя в состояние смятения и паники, не дают трезво обдумать ситуацию (роковая ошибка!), вынуждают подчиниться их указаниям и, тем самым, совершить ошибку. Фишинговые сообщения, как правило, рассылаются от банков, органов государственной власти (судебные приставы, налоговая служба, суды и т.д.) либо интернет-сервисов (почтовых сервисов (gmail.com, yandex.ru, mail.ru и других), облачных хранилищ (DropBox, Google Диск и т.д.) или сайтов онлайн-объявлений (avito.ru, hh.ru и других)).

В следующей части мы рассмотрим некоторые другие разновидности многоликого фишинга.