Многоликий фишинг (Часть 3)

Вопреки распространённому мнению, фишинг это не только поддельные email-сообщения и сайты. Каналы коммуникаций злоумышленника с потенциальной жертвой, в принципе, могут быть любыми – электронная почта, приложения для мгновенного обмена сообщениями («аська», Skype и т.п.), телефон или даже обычная (неэлектронная) почта. В этой, заключительной, части цикла про фишинг мы как раз и рассмотрим примеры использования для фишинга иных каналов, кроме электронной почты.

Возьмём, к примеру, Skype. Это приложение активно используется миллионами пользователей по всему миру, многими для деловых контактов, а потому не могло не привлечь внимание злоумышленников. В профилях пользователей Skype можно найти массу персональных данных (имя, дату рождения, адреса электронной почты, телефоны и т.д.). Лакомая цель - собранные персональные данные можно использовать для целевого фишинга.

Однажды вы получаете в Skype запрос на добавление в «контакты» от неизвестного пользователя, в котором, кроме того, содержится сообщение о том, что вы получили новое персональное сообщение и его можно посмотреть на некоем, указанном тут же в сообщении, но незнакомом вам, сайте. Если нажать на ссылку, будет предложено скачать файл-«видеоплеер», который на самом деле является вредоносным ПО, запрашивающим у пользователя права администратора компьютера и, в случае предоставления таковых, ворует персональные данные, скачивает и устанавливает на компьютер загрузчик рекламных сообщений и включает компьютер в так называемую «ботнет» - сеть компьютеров-«зомби», используемых во вредоносной деятельности в интернете без ведома владельцев таких компьютеров.

Разумеется, есть и другие примеры фишинга с помощью Skype, однако, всем им можно успешно противостоять, если помнить базовые правила:

1. Не открывать незнакомые файлы (вложения) и ссылки;
2. Регулярно обновлять базу антивируса.

Телефонный фишинг обычно используется для целевых фишинг-атак наряду с email-фишингом и иными методами. Телефонный фишинг можно отнести к довольно дорогим методам мошенничества - чтобы умело «развести» жертву, злоумышленник должен быть хорошим психологом и актёром, а это требует подготовки и опыта. Да и сама подготовка атаки, сбор данных о жертве и её окружении и разработка сценария атаки, довольно дорога и занимает время. Но и противостоять такой целевой атаке неподготовленной жертве намного сложнее – хорошо поставленная атака, проводимая опытным психологом, почти не оставляет шансов на защиту.

Примеры фишинга «по переписке» (то есть с использованием обычной почты) можно пересчитать по пальцам руки – понятно, что такой путь злоумышленников к логинам-паролям и прочим целям чрезвычайно долог, а потому сам метод неэффективен.

Подводя итог нашему краткому экскурсу в «мир» фишинга, ещё раз хотим подчеркнуть, что главное оружие против фишинга – здравый смысл и внимательность. Когда кто-то, особенно незнакомый, просит вас что-либо сделать – на это всегда полезно смотреть через «призму» его мотивации, то есть задать вопрос «зачем (или почему) он просит меня это сделать?». Но даже если причины понятны и кажутся резонными, необходимо проявлять должную внимательность и обращать внимание на такие признаки фишинговых сообщений, как поддельный адрес отправителя, отсутствие персонализированного обращения к вам, а также наличие речевых, грамматических и орфографических ошибок.

Соблюдение данных, в общем-то, простых правил, наряду с актуальным антивирусным ПО, убережёт вас от абсолютного большинства проблем, являющихся следствием фишинга.