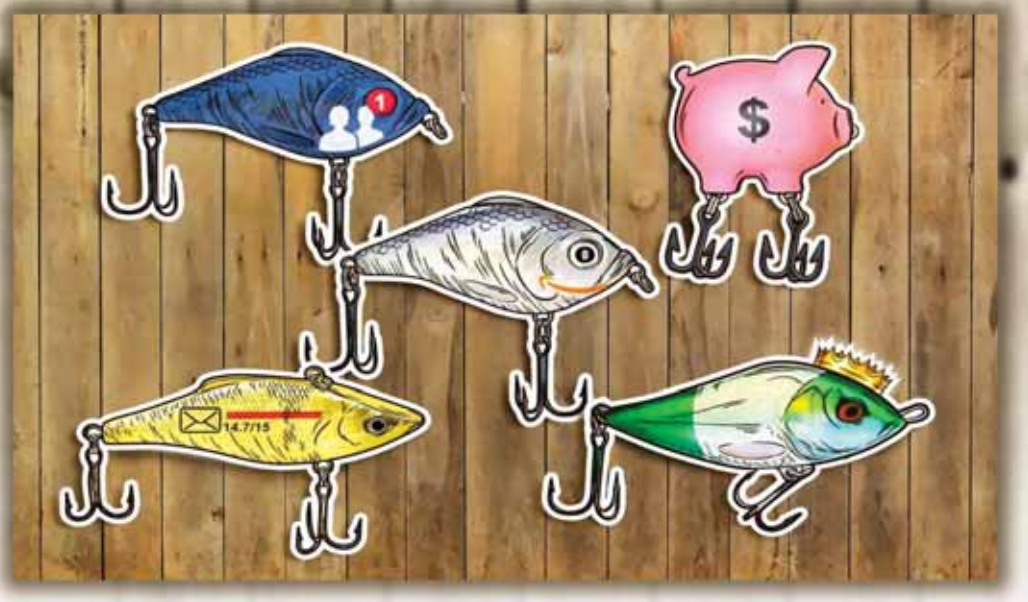


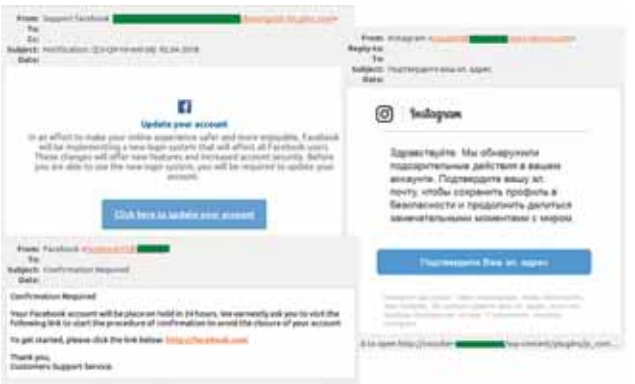
Обман в Интернете: 5 типичных приемов спамеров

Спам и фишинг зачастую неотделимы: мошенники массово рассылают письма, в которых пытаются, так или иначе, выудить у вас какую-нибудь информацию. Личные данные пользователей остаются для них самым ценным и желанным видом добычи — об этом свидетельствуют как постоянные громкие публикации в СМИ, так и наш собственный анализ спам-потока. Одна из главных тем в спаме — почтовый фишинг с использованием различных методов социальной инженерии, цель которого — заполучить доступ к вашим аккаунтам или номера банковских карт. В этой публикации мы расскажем про пять самых распространенных уловок, при помощи которых спамеры пытаются вас обмануть.

1. Поддельные уведомления от соцсетей

Спамеры активно рассылают поддельные уведомления от имени популярных соцсетей — о новых друзьях, их активностях, комментариях и лайках. Такие сообщения, как правило, почти ничем внешне не отличаются от настоящих, но содержат фишинговую ссылку, заметить которую не всегда легко. По ссылке пользователю предлагают зайти в свой аккаунт, введя логин и пароль на поддельной странице авторизации.

Другой распространенный вариант на ту же тему — письма от лица все тех же соцсетей, но уже с угрозами: либо с вашим аккаунтом якобы совершались какие-то подозрительные действия, либо просто соцсеть вводит новые функции и блокирует клиентов, не подтвердивших свое согласие. В любом случае в письме будет кнопка со ссылкой на фишинговую страницу, где вас попросят авторизоваться.



1. Популярные заходы в фишинговых письмах: поддельные уведомления от соцсетей

2. Банковский фишинг

Фишинг, направленный на получение данных банковских карт пользователей, — по-прежнему самый популярный вид мошенничества. Поддельные письма рассылаются от имени как банков, так и платежных систем. Наиболее популярные темы сообщений связаны с блокировкой счета или «подозрительной активностью» в личном кабинете клиента.

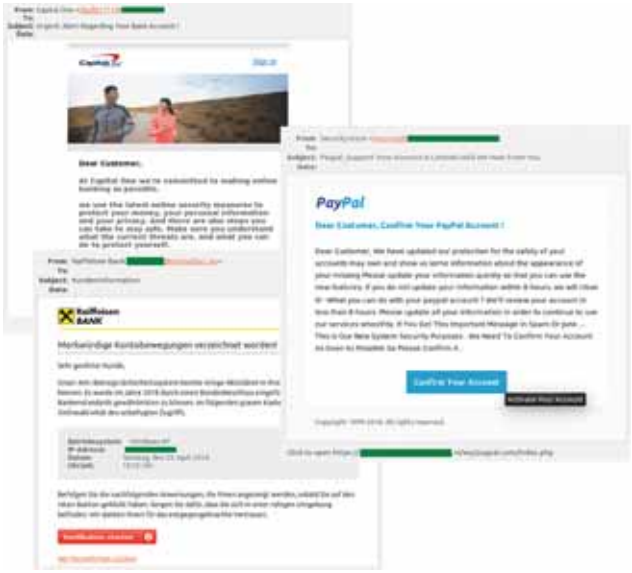
Под предлогом восстановления доступа, подтверждения личности или отмены некоторой транзакции, пользователя просят ввести данные банковской карты (зачастую вместе с CVV/CVC-кодом) на поддельной странице банка. Получив эти данные, мошенники незамедлительно выводят деньги со счета жертвы. С платежными системами то же самое — но там злоумышленники просят всего лишь войти в аккаунт.

3. Поддельные уведомления от популярных сервисов и продавцов

По такому же принципу создаются и поддельные уведомления от имени популярных магазинов, а также от сервисов доставки посылок, бронирования жилья и авиабилетов, мультимедийных развлечений, поиска работы и прочих востребованных в сети услуг. При рассылке такого спама очень высока вероятность, что сообщение попадет к реальному пользователю упомянутой услуги, а тот среагирует на тревожное уведомление и перейдет по мошеннической ссылке — на это и делают ставку мошенники.

4. Подделки под почтовые сервисы

При помощи такого рода спама мошенники собирают логины и пароли от почтовых сервисов. Здесь чаще всего используется один из двух предлогов — вам предлагают либо восстановить пароль, либо увеличить доступное место для



2. Популярные заходы в фишинговых письмах: поддельные уведомления от банков и платежных систем

3. Популярные заходы в фишинговых письмах: поддельные уведомления разнообразных сервисов и магазинов

4. Популярные заходы в фишинговых письмах: поддельные уведомления от почтовых сервисов

5. Популярные заходы в фишинговых письмах: нигерийское мошенничество

хранения писем, поскольку ваш ящик якобы забит уже целиком. В последнем случае переход по фишинговой ссылке обещает многократное увеличение лимитов, что сейчас, в эпоху облачных сервисов и постоянно растущих потребностей в хранении больших объемов данных, действительно практикуют многие компании, — в результате фишинг не кажется таким уж подозрительным.

5. Нигерийское мошенничество

Наконец, по-прежнему остается актуальным один из старейших видов спама — обещания богатств и пожертвований от имени родственников и адвокатов покойных миллионеров или политиков. Сценарий таких сообщений стандартный: мошенник обещает жертве внушительное вознаграждение, если та согласится помочь незадачливому наследнику вывести средства, застрявшие на счетах. Для этого, разумеется, нужно сначала отправить подробную информацию о себе (паспортные данные, данные о счетах и тому подобное) и некоторую сумму денег на оформление всех необходимых документов.

На этом список излюбленных спамерами методов и тематик развода не заканчивается, однако пять перечисленных выше способов — самые часто встречающиеся и, видимо, самые действенные.

Как не стать жертвой мошенников

В целом надо просто быть внимательным. Но это слишком общий совет, так что вот немного конкретики:

- Когда вы получаете письмо с уведомлением от какого-то сервиса, убедитесь, что оно действительно отправлено с адреса, принадлежащего этому сервису. Например, если речь про Google, то письмо должно прийти от no-reply@accounts.google.com, а не от no-reply@accounts.google.scroogle.com или чего-нибудь в таком духе.
- Если вы нажимаете в таком письме на ссылку — опять-таки удостоверьтесь, что вы действительно попали на сайт сервиса, а не на поддельный сайт.
- Используйте надежное защитное решение с защитой от спама и фишинга — оно распознает мошеннические письма и вовремя предупредит вас.

Источник:
www.kaspersky.ru/blog