На крючке

Текст: Наталья Югринова

Термин «фишинг» пришёл к нам из английского, где он звучит точно так же как и слово «рыбалка» (fishing), хотя пишется немного по-другому (phishing). Схожесть не случайна. В роли «рыбаков» в фишинге выступают кибермошенники, «наживкой» служат поддельные электронные письма, вебсайты и СМС. А «улов» — конфиденциальные данные незадачливых пользователей, открывающие доступ к их счетам. Как не попасться на удочку преступников?

В феврале 2019 года корпорация Microsoft опубликовала отчёт по угрозам безопасности в интернете. Выяснилось, что самым распространённым в мире способом обмана пользователей является фишинг — кража персональных данных в интернете с помощью разнообразных подставных сообщений. Количество фишинговых атак год от года увеличивается. От них почти не спасают антивирусы, фаерволы и спам-детекторы. Как объясняют аналитики Microsoft, хакеры нацеливаются на самое уязвимое звено в системе информационной безопасности — человека. Они используют методы социальной инженерии, то есть играют на эмоциях, страхах и рефлексах, чтобы заставить пользователя выполнить нужное им действие.

На крючок попадаются, конечно, не все, но значительное количество адресатов. В исследовании компании ProofPoint «State of the Phish 2019» говорится, что примерно каждый десятый нажимает на присланную ему в письме или СМС вредоносную ссылку. Около 4% пользователей вводят на поддельных сайтах свои логины, пароли, CVV-коды и другие персональные данные. Преступники обычно вылавливают добычу, раскидывая сети максимально широко: они совершают рассылки на сотни тысяч адресов. От каждой атаки, таким образом, страдают тысячи человек.

4%

пользователей

попадаются на удочку мошенников: вводят на поддельных сайтах свои логины, пароли, CVV-коды и другие персональные данные

Потери от фишинга довольно велики. В 2018 году, по сведениям российской IB-Group, только с помощью веб-фишинга (кроме него существует ещё СМС- и телефонный фишинг) в России было похищено свыше 250 млн рублей. Ущерб от одной атаки на пользователя варьируется от 2 до 50 тыс. рублей. Не весь фишинг направлен на получение доступа к финансовым счетам пользователей. Иногда злоумышленники выуживают логин и пароль от аккаунтов в социальных сетях — в том числе для вымогательства денег у владельца или его друзей. Некоторые подписывают пользователя на платные услуги или рассылки без его ведома. Другие «перехватывают» деньги при переводе с карты на карту или при попытке заплатить за услуги операторов сотовой связи.

«Наживка», которую используют фишеры

Источник: ProofPoint

Все инструменты фишинга можно разделить на три категории:

1. Фальшивые веб-сайты, которые имитируют реальные интернет-ресурсы, — например, mïcrosoft.com (используется латинская i с умлаутом) вместо microsoft.com или sber.ru вместо sberbank.ru.

2. Почтовые рассылки, СМС или сообщения в соцсетях со ссылками на фишинговые сайты, где вас просят пройти идентификацию и ввести личные данные.

3. Рассылки с вредоносными вложениями: кликнув на них, пользователь активирует установку вируса на своё устройство.

По данным ProofPoint, подавляющее большинство атак (69%) осуществляется при помощи электронных писем. На веб-сайты приходится 17% атак, на вложения с вирусами — 14%.

Особенности национальной «рыбалки»

Методы фишинговых атак хорошо известны и с годами существенно не меняются. Если изучить, как действуют мошенники, то можно понять, на какие детали стоит обратить внимание при работе в интернете. Как правило, «рыбаки» руководствуются следующей стратегией.

Сначала выбирается жертва. Большинство злоумышленников рассылают сообщения наугад — по крупным базам email-рассылок и телефонных номеров. В таких письмах и СМС к пользователю обращаются обезличенно: «Уважаемый клиент» или просто «Здравствуйте!». В последнее время практикуются и более персонализированные атаки: для убедительности к адресату обращаются по имени-отчеству. Нужно помнить, что имя, отчество и фамилия, возраст, регион проживания и другие детали легко получить из соцсетей или баз данных, которые продаются повсеместно.

Затем в дело вступает социальная инженерия — тонкое, требующее знания психологии умение манипулировать чувствами человека. Кибермошенник может притвориться представителем крупного банка, телеком-оператора, бизнес-партнёра, службы экспресс-доставки. Либо выдумать «своего» персонажа — учёного-исследователя, рекрутёра, страховщика, студента, красавицу-блогершу и т. д. Его задача — составить послание с таким текстом, чтобы прочитавший его человек как можно скорее кликнул на приложен-

250

млн рублей

составила добыча веб-фишеров в 2018 году, по оценкам IB-Group

ную ссылку или открыл вложение. Ссылка, как правило, ведёт на фишинговый сайт. Само сообщение тоже старательно мимикрирует под настоящее. Прошли те времена, когда фишинговое письмо легко было определить по орфографическим ошибкам и хромающей стилистике. Сейчас хакеры компонуют их из подлинных сообщений и поэтому почти не делают ошибок.

И, наконец, готовится техническая инфраструктура для того, чтобы «подсечь рыбку». «Рыбаки» расставляют свои сети там, где вы этого не ожидаете. Они могут взломать точку доступа к общественной сети Wi-Fi и подменить адрес сайта, где происходит авторизация пользователя, на поддельный. Фишинговый сайт может быть почти полностью идентичным официальному сайту компании, от лица которой ведётся переписка: тот же логотип, фирменные цвета, контент. Доменное имя может быть очень похожим на оригинал или даже полностью совпадать с ним. Подозрительным сигналом в этом случае должно стать то, что фишинговый вебсайт работает без SSL- и TLS-сертификата, по незащищённому протоколу HTTP, в то время как официальные организации пользуются защищённым HTTPS. Мошенники не только создают фишинговые сайты, но и активно их продвигают в соцсетях и поисковых системах. Если речь идёт о вредительских вложениях к «письмам счастья», их тоже тщательно маскируют. Они могут выглядеть как безобидный документ (например, «Счёт_17.doc», «Ведомость.xls» или «Договор_займа.pdf») либо обычный файл формата zip, rar, exe и др.

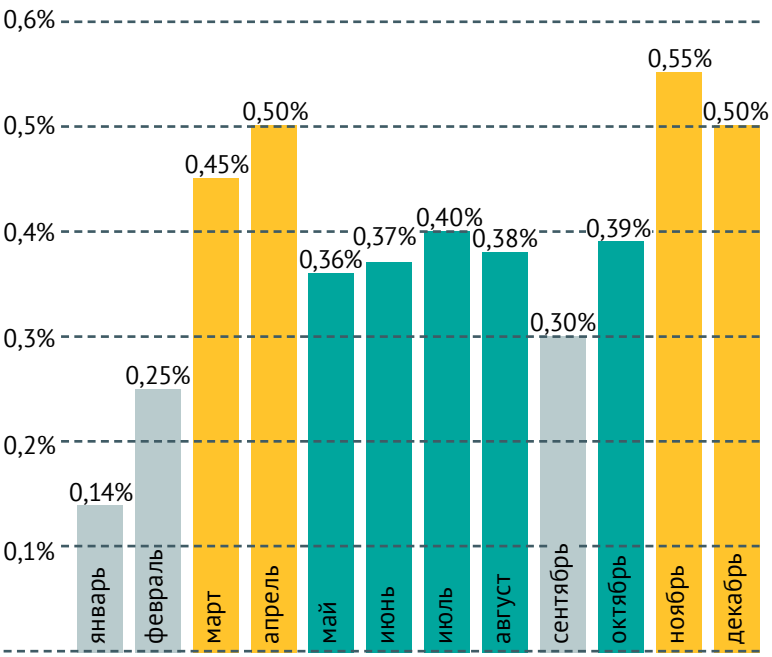
Как отмечают в компании IB-Group, порог входа в криминальный бизнес фишинга очень низкий. Если для организации хакерской атаки на корпорации необходимо сколотить профессиональную группу, то фишингом нередко промышляют айтишники-одиночки. На хакерских форумах недорого продаются специальные программы — конструкторы фишинговых сайтов, позволяющие поставить криминальный промысел на поток. Относительная простота организации преступных схем и массовость охвата делают фишинг вдвойне социально опасным.

Мастера перевоплощения

Раз в три месяца американская компания KnowBe4 проводит исследование Top-Clicked Phishing Email Subjects («Самые кликабельные темы в фишинговых рассылках»). Она рассылает миллионам пользователей «фальшивые» фишинговые письма, чтобы проверить, на какие обращения они клюнут, а на какие — нет. В первом квартале 2019 года самыми популярными сообщениями, на которые отзывались пользователи, оказались письма от лже-LinkedIn с темами «Присоединись к моей сети контактов» и «Ваш профиль просмотрели», а также от лже-Facebook с предупреждением о смене пароля и привязанного адреса электронной почты. «Хакеры играют на ваших чувствах, — говорится в отчёте. — Вы читаете заголовок о том, что кто-то получил доступ к вашему аккаунту, и немедленно начинаете паниковать. Важно решить проблему как можно быстрее. В стрессовой ситуации ваше внимание притупляется. Этим и пользуются преступники».

Как мошенники отключают критическое мышление адресата? Представьте, вам приходит письмо от «банка» такого содержания: «На ваше имя был оформлен потребительский кредит через он-

Доля фишинговых посланий в общем объёме входящих email в 2018 году



Источник: Microsoft

лайн-банкинг на сумму 427 998 рублей. В настоящее время задолженность не погашена. На 15.05.2019 ваш долг с учётом пени составляет 633 733 рубля. В связи с этим был составлен судебный иск. Пожалуйста, ознакомьтесь с документами во вложении». Естественно, первая реакция — удивление. Какой кредит? Это какая-то ошибка! Но вместо того, чтобы звонить в банк и выяснять, в чём дело, вы кликаете по ссылке на приложенные «документы».

Иногда тактика меняется: вас не запугивают, а, наоборот, манят перспективой получить выигрыш, новую работу, денежный перевод. На «пряник» мозг реагирует почти так же, как и на «кнут», — затуманивается. Например, вам приходит СМС с информацией о том, что вы выиграли автомобиль в конкурсе от вашего оператора сотовой связи. От вас требуется только одно — перейти по ссылке и ввести свои данные или отправить ответное сообщение на короткий номер. Малая плата за большой приз, не так ли? Вы даже не отдаёте себе отчёта в том, что выиграть что-либо можно, лишь приняв участие в конкурсе. А конкурсов вида «Перейдите по ссылке и получите подарок» просто не существует. Под видом подарка могут предлагать что угодно: дешёвые авиабилеты, золотые карты лояльности торговых сетей, скидки от компаний-партнёров… Традиционный всплеск фишинговых атак происходит во время «чёрной пятницы» и сезона новогодних распродаж: письма выдаются за акции магазинов и поздравления. Насторожить вас должно то, что все эти предложения заканчиваются подозрительным призывом к срочному действию.

Фишинговые атаки могут происходить с помощью обычного телефона — для их обозначения придумали даже специальный термин «вишинг» (от англ. voice и phishing, то есть «голосовой фишинг»). Схема в целом та же: мошенник звонит своей жертве и представляется сотрудником банка, налоговой или другого официального органа. Затем он сообщает о какой-то проблеме — ошибке в счетах, краже средств с карты, неоплаченном штрафе. Решить проблему нужно немедленно, и для этого требуется сообщить свои данные или код подтверждения, который придёт на телефон (подробнее о телефонных мошенничествах читайте в статье «Телефон недоверия» в выпуске №2 журнала «Дружи с финансами»). Растущая популярность вишинга связана с тем, что на телефонные звонки даже с незнакомых номеров отвечает более 90% пользователей. А вот электронные письма от неизвестных отправителей открывает, по статистике, лишь каждый третий.

Безопасная сеть

Универсальное «лекарство» от фишинга — внимательность и осторожность при работе в интернете, особенно при обращении с финансами. Вот несколько правил, которые помогут всегда оставаться начеку и не попасться на удочку мошенников.

Всегда внимательно проверяйте ссылку, по которой собираетесь кликнуть. Перед адресом сайта в строке URL обязательно должен стоять префикс https: он означает, что соединение безопасное. Не вводите свои конфиденциальные данные на сайтах с префиксом http.

Получив подозрительное письмо или СМС от незнакомого отправителя, внимательно проверяйте текст, логотипы, вложения — особенно если в сообщении есть призыв к немедленному действию. Наведите курсор на гиперссылку: так вы узнаете, действительно ли она ведёт туда, куда обещает название.

Кибермошенники используют методы социальной инженерии, то есть играют на эмоциях, страхах и рефлексах, чтобы заставить пользователя выполнить нужное им действие

Аккаунты людей, с которыми вы знакомы лично, тоже могут взломать. Насторожитесь, если старый приятель вдруг начинает разговор в соцсетях с просьбы перевести ему денег. Лучше позвоните ему и убедитесь, что просьба действительно исходит от него.

Не заходите в онлайн-банки и другие финансовые сервисы через публичный Wi-Fi — в кафе, общественном транспорте, на улице. Лучше воспользуйтесь мобильным интернетом.

Обнаружив фишинговое письмо или сайт, сообщите о нём в организацию, которую оно компрометирует. Если письмо пришло от имени банка, напишите о нём в сам банк, если от соцсети — отправьте в её службу поддержки. Это поможет быстрее выявить и остановить мошенников.