ЕВГЕНИЙ ПАВЛЕНКО

щений в надежде попасть на клиента Сбербанка) премию. Чтобы ее получить, достаточно положить средства на свой мобильный телефон через терминал Сбербанка. При этом средства предлагается перевести на электронный кошелек, номер которого идентичен номеру мобильного телефона данного клиента. Не обладающий необходимой финансовой грамотностью человек уверен, что кладет средства на свой счет мобильного телефона. Однако в итоге перечисляет их на электронный кошелек злоумышленника.

Жертвы активного общения

Достаточно много людей по долгу службы ведут активную переписку и вынуждены открывать все входящие письма — те же сотрудники отдела кадров, менеджеры по продажам и т. д. Часто почтовые адреса данной категории лиц есть в открытом доступе на сайте. На них и на других лиц, активно общающихся по электронной почте, нацелены атаки с использованием так называемых фишинговых писем.

Фишинг — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

В подобных письмах обычно содержится либо вложение с вредоносным вирусом, либо ссылка на сайт, где будет расположен вредонос. Наиболее яркий пример использования подобной технологии — атаки на банки хакерской группировкой Cobalt, которая похитила со счетов в 2017 году более 1 млрд руб. Злоумышленники делали веерные рассылки фишинговых писем, содержащих вредонос, сотрудникам банков в надежде, что кто-либо откроет файл. Схожие методы используют мошенники, выводящие средства через банки-клиенты компаний.

По данным «Лаборатории Касперского», в 2017 году 16% всех пользователей электронной почты столкнулись с фишингом, доля спама в почтовом трафике составила более 56%.

Интернет-серферы

Активные пользователи сети Интернет также под угрозой. Для них злоумышленники подготовили фишинговые сайты, чаще всего мимикрирующие под сайты кредитных организаций. После того как пользователь попадает на такой сайт, мошенники пытаются побудить пользователя оставить свои персональные данные, получить доступ к аккаунтам, банковским счетам или заразить вредоносом, с помощью которого впоследствии может быть совершено хищение.

По данным «Лаборатории Касперского», в 2017 году фишинг в интернете стал еще более скрытным, отличить мошеннические сайты от настоящих все сложнее. Например, еще год назад наличие SSL-сертификата (присутствие HTTPS в адресной строке) было гарантией подлинности сайта, тогда как в 2017 году многие фишинговые сайты имели все сертификаты. Кроме этого, фишинговые страницы часто располагаются на взломанных легальных сайтах. «Такие странички порой удачно маскируются, и даже после того, как пользователь вводит свои учетные данные, его автоматически перебрасывают на страницу оригинального сервиса с просьбой авторизоваться повторно по причине технического сбоя,— рассказывает руководитель экспертного центра безопасности Positive Technologies Алексей Новиков.— Таким образом, у пользователя не возникает подозрений, что его данные были введены в некорректном месте».

Group-IB 2017 году предупреждала о массовом заражении вирусом Bulgar вполне легальных новостных сайтов, а также сайтов для бухгалтеров и юристов, что позволяло незаметно для клиента похищать деньги у него или у компании, где он работал. В одном из подобных кейсов с момента захода клиента на бухгалтерский сайт до хищения прошло всего 13 минут.

Криптовалютчики

В прошлом году мошенники, использующие социальную инженерию, активно интересовались криптовалютами. Эксперты Positive Technologies отметили, что в этой сфере применялись самые разные методы. Например, воздействовали на членов команды ICO-проектов: для похищения электронной почты организатора ICO запрашивали восстановление пароля, а затем меняли. Подспорьем для мошенников является открытость компаний: адреса электронной почты и ФИО сотрудников есть на веб-сайте ICO.

Информации из социальных сетей зачастую достаточно, чтобы определить логин электронной почты, а затем восстановить от нее пароль.

Практически все крупные криптовалютные биржи стимулируют пользователей к использованию двухфакторной аутентификации. Однако значительное количество пользователей ее так и не включают. При использовании СМС-сообщений в качестве второго фактора они могут быть похищены при помощи атак на каналы связи либо выкуплены на черном рынке. И этим фактом пользуются мошенники, чьей целью является криптовалюта.

Например, в 2017 году произошел яркий случай воровства криптовалюты, когда хакер убедил сотрудников сотовых операторов перенести номер жертвы на свою сим-карту. Еще один известный случай, когда злоумышленники использовали фишинговые вебсайты, имитирующие настоящий домен Binance (крупнейшей криптовалютной биржи).

На те же грабли

Вариаций мошенничеств, где атаки на пользователей идут с использованием социальной инженерии, такое количество, что все больше людей становятся жертвами злоумышленников повторно, предостерегают эксперты. «Наша статистика говорит о том, что в регионах очень высок процент повторяемости инцидентов с одними и теми же людьми,— сетует директор центра мониторинга и реагирования на кибератаки Solar JSOC компании Solar Security Владимир Дрюков.— Один из 25 пользователей, которые стали жертвами злоумышленников и скомпрометировали данные своих банковских карт, в течение полугода наступит на те же грабли». Это говорит о низком уровне осведомленности жителей России о базовой гигиене информационной безопасности, подытожил он. ●

КАК БОРОТЬСЯ

В борьбе с мошенниками, использующими социальную инженерию, спасение утопающих — дело рук самих утопающих. Есть несколько простых правил, которые следует соблюдать.

1. Никому и никогда не сообщать паролей для входа в онлайн-банк, номер банковской карты, CVC-код и иную информацию, позволяющую произвести списание. Даже если позвонивший представится сотрудником банка и будет иметь о вас какую-то информацию (знать ФИО, дату рождения и т. д.).
2. Вы всегда должны быть точно уверены, что разговариваете именно с сотрудником банка, МФО и т. д. Не уверены — перезвоните самостоятельно в банк, в МФО. Например, в случае возможных проблем с банковской картой лучше звонить по телефонам, указанным на обороте карты.
3. Не открывайте сообщения и не переходите по ссылкам от незнакомых лиц. Даже если от знакомого приходит неожиданное сообщение (например, от малознакомого коллеги — текст типа «приколись, как я отрываюсь») — уточните, действительно он направлял вам это сообщение или же его почтовый ящик был взломан.
4. То же касается сообщений в соцсетях — если друг просит денег взаймы или пополнить ему телефон, убедитесь, что просьба исходит от друга, а не от взломавшего его аккаунт злоумышленника.
5. Кроме этого, очень важно быть в курсе, какие угрозы, связанные с социальной инженерией, вас подстерегают. А для этого необходимо читать публикации, посвященные этому вопросу, в том числе о новых методах злоумышленников.