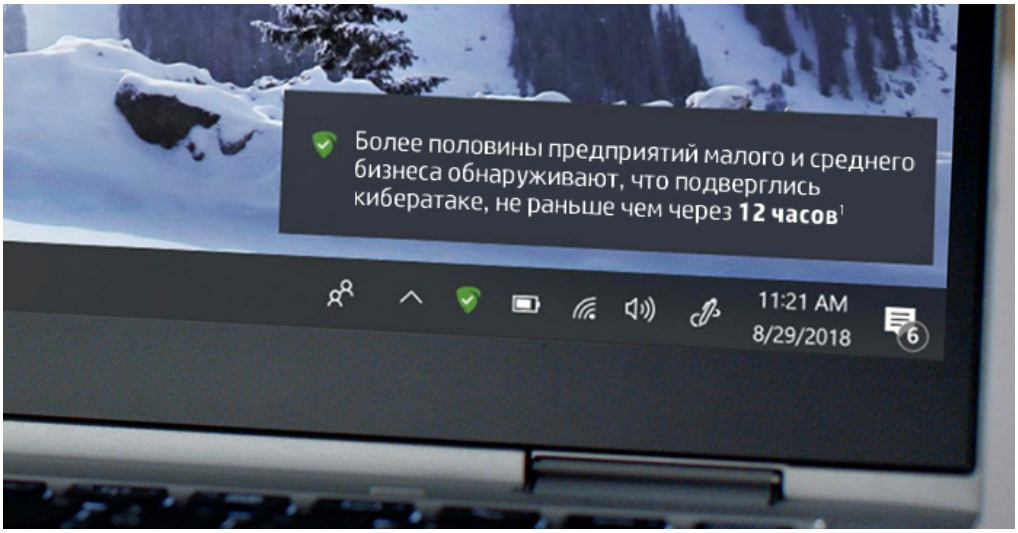
Теперь фишинг угрожает не только электронной почте

Подробнее



Веб-браузер — это портал в мир информации… и угроз. Что же можно предпринять для защиты своего бизнеса?

Веб-браузеры отвечают за многое. Недавний опрос, проведенный среди 400 директоров по информационным технологиям, показал, что 68 % считают современных киберпреступников настолько изобретательными, что сотрудникам трудно отличить безопасный сайт от небезопасного[2]. Поэтому неудивительно, что около 70 % ИТ-специалистов еженедельно сталкиваются с фишинговыми атаками — и не только по электронной почте[3]. Сегодня изобретательные хакеры используют социальные сети, рекламу и распространенные опечатки при вводе адресов веб-сайтов, чтобы заставить сотрудников компаний раскрыть конфиденциальную личную информацию. Поскольку фишинговые аферы все сложнее вычислить, компании прилагают огромные усилия для защиты своих сотрудников от этих атак.

Несмотря на информирование об угрозах и инвестиции в обучение сотрудников и ПО для обеспечения безопасности, количество кибератак на ноутбуках и настольных компьютерах выросло более чем на 100 %[4]. Киберпреступники по-прежнему прорываются через защитные барьеры, поскольку на их стороне количественное превосходство. Защита данных требует огромных усилий, а чтобы поставить бизнес под угрозу, достаточно лишь одного сотрудника, перешедшего по зараженной ссылке.

Значительную часть этой проблемы составляют кибератаки в социальных сетях. Такие платформы, как Facebook и Twitter, — настоящее раздолье для киберпреступников. Они не только созданы для взаимодействия и коммуникации, но также просты в использовании, и их содержание обходится недорого. Невероятно просто создать фальшивый аккаунт и начать размещать вредоносное содержимое — от ссылок и сбора данных до целевых страниц и ненадежных всплывающих окон.

Большая часть этих действий в Интернете основаны на фишинговых техниках, которые раньше использовались только для электронной почты. Социальные сети предназначены для того, чтобы люди могли связываться друг с другом, поэтому не составляет никакого труда создать солидный надежный образ и приобрести подписчиков среди настоящих пользователей платформы.

Для большинства компаний, ставших жертвами фишинговых атак, последствия могут оказаться разрушительными и с далеко идущими последствиями. Помимо снижения продуктивности сотрудников и утечки данных клиентов, результатом такой атаки может стать потеря самих клиентов. Нарушение безопасности может свести на нет доверие клиентов к вашему бизнесу: для них вы больше не будете надежным источником информации. Конечно, ситуацию можно исправить, однако чаще всего последствия оказываются неустранимыми.

Теперь фишинг угрожает не только электронной почте

В 4-м квартале 2017 г. уровень фишинговых атак в социальных сетях взлетел на 500 %, а основной их тенденцией стало создание фальшивых аккаунтов, которые представляются как клиентская поддержка крупных брендов[5]. Эта разработка получила название angler-phishing («выуживание»), поскольку хакеры забрасывают наживку и ждут, когда пользователи социальной сети клюнут на нее. Используя ту же фирменную символику и аутентично выглядящее имя аккаунта, мошенники обманывают миллионы людей, которые доверяют социальной сети. После того, как пользователь «клюнул», с фальшивого аккаунта ему отправляется ссылка на фишинговый сайт, где пользователю предлагают зарегистрироваться, что позволяет фишинговому мошеннику получить доступ к его личным данным.

Один из способов защиты от фишинговых атак через социальные сети — изменить модель поведения ваших сотрудников. Это поможет им избежать простых ошибок, влекущих разрушительные последствия для вашего бизнеса.

1. Взаимодействуйте только с теми пользователями, которым можно доверять.
2. Не переходите по ссылкам из непроверенных источников.
3. Никогда не загружайте прикрепленные файлы из социальных сетей.
4. Включите двухфакторную аутентификацию на всех устройствах и аккаунтах социальных сетей: так их будет сложнее взломать.
5. Проводите дополнительный инструктаж среди сотрудников с более высокими правами доступа или социальными ролями.

Другим важным аспектом плана обеспечения безопасности являются технологии, которые компания использует для защиты от кибератак. Например, ноутбуки, настольные компьютеры и рабочие станции семейства HP Elite изначально разрабатывались для обеспечения максимального уровня безопасности.

Одной из таких функций безопасности является HP Sure Click[6], доступная на некоторых ноутбуках и рабочих станциях HP Elite, которая обеспечивает совершенно другой подход к обеспечению безопасности поиска в Интернете. Вместо того, чтобы просто отмечать опасные сайты как нежелательные, эта функция также препятствует заражению других вкладок и всей системы вредоносным ПО, программами-вымогателями и вирусами. HP Sure Click запускается для каждого сайта, который посещает пользователь. При каждом посещении определенного веб-сайта HP Sure Click создает изолированный на уровне аппаратного обеспечения сеанс просмотра, в рамках которого этот веб-сайт не может заразить другие вкладки или саму систему.

HP Sure Click защищает пользователей даже от зараженного вредоносного ПО, скрытого в документах Office и PDF-файлах. Предположим, ваши сотрудники получают зараженный PDF-файл в сообщении электронной почты. Они могут совершенно спокойно открыть файл, зная, что HP Sure Click изолирует вирус на аппаратном уровне и предотвратит распространение заражения за пределы файла. Благодаря этому решению для обеспечения безопасности, встроенному в парк компьютерного оборудования, вы можете больше не опасаться интернет-угроз.

Однако изменить стратегию обеспечения безопасности и внедрить такие ультрасовременные устройства, как, например, HP EliteBook x360 с опциональными процессорами Intel® Core™ i7 8-го поколения, — не всегда так просто.
И здесь на помощь приходит HP Device as a Service (DaaS)[7]. Это современная модель потребления вычислительных устройств, благодаря которой коммерческие организации смогут экипировать своих сотрудников нужным аппаратным обеспечением и принадлежностями, управлять парком устройств с разными ОС и получать дополнительные услуги в течение срока службы этих устройств. HP DaaS предоставляет простые универсальные планы с оплатой за каждое устройство, которые обеспечат бесперебойную и эффективную работу сотрудников.

Хорошо обученный персонал и устройства, оптимизированные для обеспечения максимальной безопасности, помогут вам противостоять нарастающей угрозе киберпреступности в социальных сетях. Кибератаки будут становиться все более масштабными и разрушительными, поэтому сейчас самое время усилить оборону.

Откройте преимущества решений HP для обеспечения безопасности вашего бизнеса.

Источники:

1. Osterman Research при финансовой поддержке Malwarebytes: Second Annual State of Ransomware Report: US Survey Results (Второй ежегодный доклад о состоянии программ-вымогателей: результаты исследования, проведенного в США), июль 2017 г.
2. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
3. http://www8.hp.com/us/en/hp-news/press-release.html?id=1763561#.WLTLYjsrI2y
4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar

6. HP Sure Click доступен на большинстве компьютеров компании HP и поддерживает Microsoft® Internet Explorer, Google Chrome и Chromium™. Поддерживаемые вложения: Microsoft Office (Word, Excel, PowerPoint) и PDF-файлы в режиме только для чтения, если установлены Microsoft Office или Adobe Acrobat.

7. Планы и (или) включенные компоненты HP DaaS зависят от региона или уполномоченного сервисного партнера HP DaaS. Чтобы получить подробную информацию по вашему региону, обратитесь к местному представителю HP или уполномоченному партнеру DaaS. Услуги HP регулируются условиями и положениями HP, применимыми к предоставляемой услуге или определенными в момент покупки. Заказчик может иметь дополнительные законные права в соответствии с применимыми местными законами. Такие права не затрагиваются условиями и положениями оказания услуг HP или ограниченной гарантией HP, предоставляемой с продуктом HP.

4AA7-317RUE, апрель 2019 г.