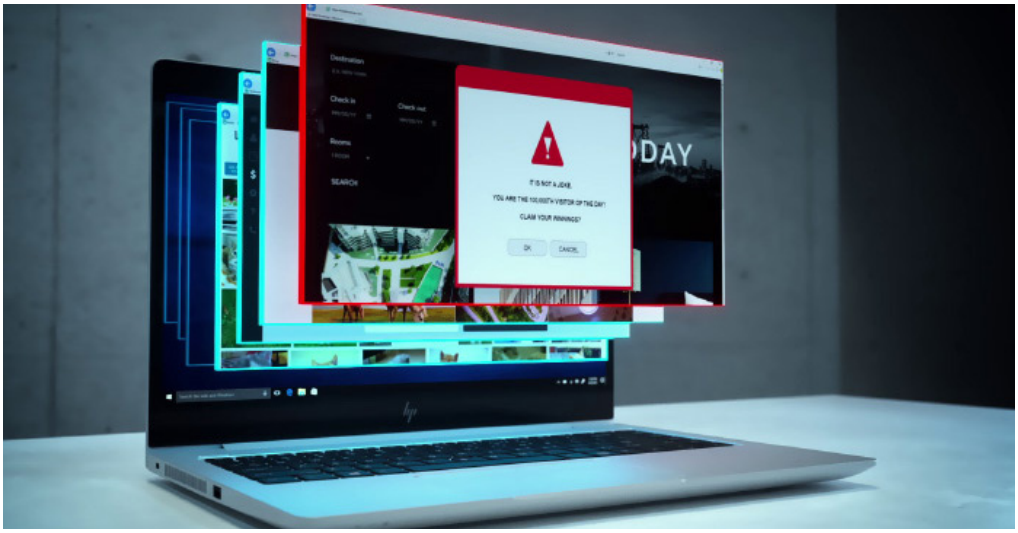
Теперь фишинг угрожает не только электронной почте

Перейти



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[1]. Поэтому неудивительно, что 70% ИТ-специалистов еженедельно сталкиваются с фишинговыми атаками – и не только по электронной почте[2]. 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 осведомленность и инвестиции в ПО для обеспечения безопасности и в обучение сотрудников, за последние шесть лет было отмечено увеличение кибератак на 232% на ноутбуках и настольных компьютерах[3]. Киберпреступники по-прежнему прорываются, поскольку на их стороне обширные бот-неты. Защита данных требует огромных усилий, но чтобы поставить бизнес под угрозу, достаточно, чтобы один сотрудник перешел 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.

Vevo – сервис потоковой передачи данных – недавно стал жертвой массовой утечки данных. Один из сотрудников компании подвергся фишинговой атаке через LinkedIn, что привело к утечке 3,12 Тбайт внутренних файлов в Интернет. Среди потерянных данных – видео, офисные документы, рекламные материалы, еще не опубликованное содержимое социальных сетей и информация об исполнителях, заключивших соглашения со звукозаписывающими компаниями[4].

Ответственность за эту атаку взяла на себя группировка хакеров OurMine после препирательства с сотрудником Vevo по электронной почте. Этот пример демонстрирует опасность **направленного фишинга** – целевой атаки, суть которой заключается в попытке украсть определенную информацию у определенной жертвы. Наиболее часто (в 91% случаев) хакеры представляются друзьями или доверенным источником (например, банком), пытаясь выудить у жертвы нужную информацию.

Теперь фишинг угрожает не только электронной почте

Для большинства компаний, ставших, как и Vevo, жертвой фишинговой атаки, последствия могут оказаться разрушительными и долгосрочными. 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.

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, мошенникам удается обмануть 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 простейших способов защиты от фишинговых атак через социальные сети – это изменение модели поведения ваших сотрудников. Это поможет вашим служащим избежать простых ошибок с разрушительными для бизнеса последствиями.

1. Взаимодействуйте только с теми пользователями, которым можно доверять.
2. Не переходите по ссылкам от 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 и компьютеры семейства HP Elite изначально разработаны для обеспечения максимального уровня безопасности.

Одной из защитных функций является HP Sure Click, доступная на некоторых платформах HP Elite, которая гарантирует безопасность 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 на каждом сайте, который посещает пользователь. При каждом посещении определенного веб-сайта HP Sure Click создает изолированный сеанс просмотра на базе аппаратного обеспечения, в рамках которого этот веб-сайт не может заразить другие вкладки или саму систему.

Однако изменить стратегию обеспечения безопасности и внедрить такие ультрасовременные устройства, как, например, HP EliteBook серии 800 с опциональными процессорами Intel® Core™ 8-го поколения, – совсем не просто. Сделать это поможет решение HP Device as a Service (DaaS). Это современная модель использования ПК, благодаря которой коммерческие организации смогут экипировать своих сотрудников нужным аппаратным обеспечением и аксессуарами, 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 укрепить оборону.

Узнать больше о защите устройств компании и преимуществах решений HP по обеспечению безопасности для вашего бизнеса.

Источники:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218RUE, Май 2018 г.