



Бренды под ударом

Мошенничество в интернете — одно из самых распространенных киберпреступлений вне зависимости от региона. При создании фишинговых и “скам”-ресурсов злоумышленники предпочитают использовать идентичность с реальными брендами, что позволяет им проводить целевые атаки на клиентов этих брендов либо привлекать потенциальных жертв за счет популярности бренда.

Около 80 процентов всех создаваемых мошеннических ресурсов эксплуатируют бренды известных компаний. Остальная часть приходится на бе-

зыманные ресурсы или придуманные злоумышленниками несуществующие бренды. Аналитики департамента по защите от цифровых рисков (Digital Risk Protection) компании F6 проанализировали фишинговые и “скам”-атаки на российские компании в первом полугодии 2025 года, основные угрозы для брендов в цифровом пространстве и тренды киберпреступности в этой сфере. При исследовании специалисты компании использовали статистику атак, заблокированных мошеннических ресурсов, которую получили при защите брендов клиентов F6.

Тенденцию к замедлению активности злоумышленников в отношении защищаемых брендов аналитики F6 связывают с экономическими причинами. Киберпреступники постепенно теряют интерес к брендам, которые находятся под защитой решения Digital Risk Protection: рентабельность атак с использованием таких брендов продолжает снижаться, в том числе из-за оперативного обнаружения и блокировки ресурсов. В то же время себестоимость атак падает на фоне развития мошеннических схем, автоматизации создания мошеннического контента и повышения доступности инструментов для совершения преступлений. Этот фактор влияет на общее увеличение количества мошеннических атак.



Рис. 1. Среднее количество фишинговых и мошеннических ресурсов, создаваемых на один бренд, по итогам первого полугодия 2025 года в сравнении с первым полугодием 2024 года

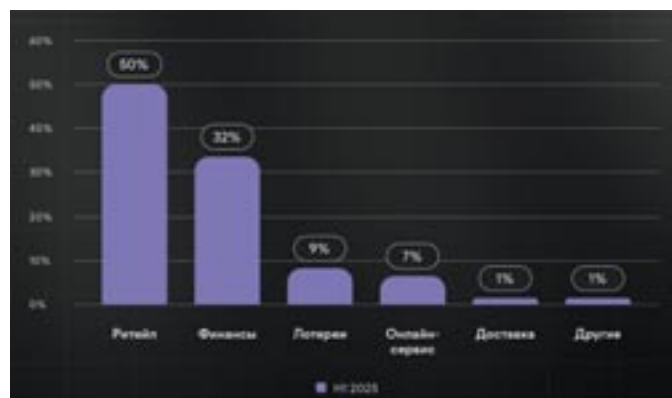


Рис. 2. Статистика фишинговых атак по отраслям по итогам первого полугодия 2025 года

зыманные ресурсы или придуманные злоумышленниками несуществующие бренды. Аналитики департамента по защите от цифровых рисков (Digital Risk Protection) компании F6 проанализировали фишинговые и “скам”-атаки на российские компании в первом полугодии 2025 года, основные угрозы для брендов в цифровом пространстве и тренды киберпреступности в этой сфере. При исследовании специалисты компании использовали статистику атак, заблокированных мошеннических ресурсов, которую получили при защите брендов клиентов F6.

Тенденцию к замедлению активности злоумышленников в отношении защищаемых брендов аналитики F6 связывают с экономическими причинами. Киберпреступники постепенно теряют интерес к брендам, которые находятся под защитой решения Digital Risk Protection: рентабельность атак с использованием таких брендов продолжает снижаться, в том числе из-за оперативного обнаружения и блокировки ресурсов. В то же время себестоимость атак падает на фоне развития мошеннических схем, автоматизации создания мошеннического контента и повышения доступности инструментов для совершения преступлений. Этот фактор влияет на общее увеличение количества мошеннических атак.

В 2025 году ритейл вышел на первое место среди отраслей, против которых чаще всего направлены действия мошенников. На него приходится 50 процентов всех фишинговых и 32 процента “скам”-атак. Долгое время основной целью оставался финансовый сектор, однако его доля снижается: по итогам первого полугодия 2025 года на банки и другие финансовые организации пришлось 32 процента фишинговых атак и столько же “скам”-активности.

Благодаря разнообразию компаний в сфере ритейла злоумышленники регулярно пополняют схему новыми шаблонами и брендами. Так, в мошеннических группах, работающих по схеме “Мамонт”, в первом полугодии 2025 года на четыре бренда из финансовой сферы приходилось 15 из ритейла — это маркетплейсы, онлайн-магазины и крупные розничные сети. Также мошенники используют их для создания фальшивых розыгрышей, акций и подарков, постоянно расширяя список задействованных брендов.

Кроме того, в схеме “Мамонт” активно используются бренды логистических компаний и онлайн-сервисов, например бронирования жилья.

Статью целиком читайте
в бумажной версии журнала