



Эволюция фишинга: от примитивных писем к deepfake и целевым атакам

Николай
Гавриченко



Аннотация

В статье прослеживается эволюция фишинговых атак от их зарождения до современности. Предлагается классификация развития фишинга по четырём ключевым этапам, согласно методам и временным периодам. Особое внимание уделяется переходу от массовых атак к целевым, основанным на социальной инженерии, и новейшим опасным трендам, таким как генерация убедительных текстов с помощью AI и подмена голоса и лица в реальном времени с помощью deepfake.

Ключевые слова:

фишинг, кибербезопасность, целевой фишинг, искусственный интеллект (AI), социальная инженерия, информационная безопасность, кибермошенничество.

Введение

Фишинг представляет собой одну из самых распространенных интернет-угроз, целью которой является получение личных данных пользователя, например, учётных данных, номера карты, кода из SMS и т.д. Методы фишинга развиваются в соответствии с техническим прогрессом.

Раньше достаточно было обращать внимание на адрес отправителя, корректность ссылок и просто орфографические ошибки. Сегодня атаки стали технологичнее, точнее и менее очевидными. Данная статья о том, как киберпреступники идут в ногу со временем, используя актуальные инструменты в связке с уязвимостями человеческой психологии.

Результаты

Эволюцию фишинга можно классифицировать по временным периодам и уровню сложности, выделив четыре основных этапа, которые отличаются методами и целями атак.

1. Примитивный массовый фишинг

На ранних этапах фишинг характеризовался массовостью и минимальной избирательностью. Злоумышленники использовали рассылки на миллионы случайных электронных почтовых адресов.

Техническая реализация была примитивной: письма часто отправлялись с бесплатных почтовых сервисов, содержали огромное количество грамматических и орфографических ошибок, а их дизайн лишь отдалённо напоминал бренды, под которые они маскировались.

Провокационные заголовки, а также явная подделка известных URL позволяли легко определять нежелательную рассылку. Согласно статистике, эффективность таких атак составляла менее процента, но с учётом количества писем фишинг приносил значительный доход.

Реальный случай: «Нигерийские письма» или «письма счастья». Пользователь мог получить письмо с заголовком «Срочно! Помогите получить наследство!» В тексте некая «Мария Джонсон» из Лондона рассказывала трогательную историю о миллионах долларов, замороженных на счёте её покойного мужа, и просила помочь с переводом денег в обмен на 10% от суммы. Для получения средств требовалось «всего лишь» предоставить данные банковского счёта и оплатить небольшие «законные издержки». Другой распространённый пример — письма от имени «службы безопасности» eBay или PayPal с грубыми ошибками в логотипе и тексте, требующие «проверить учётную запись» по ссылке, ведущей на сайт paypal-security.com.

2. Технологический фишинг

С повышением общей осведомлённости пользователей, а также развитием спам-фильтров и антивирусного программного обеспечения киберпреступники стали адаптироваться и применять более серьёзные инструменты [1].

Значительно выросло качество исполнения. Злоумышленники создавали полноценные сайты, копирующие дизайн и логику (например, авторизацию) оригинального ресурса.

Электронные письма подкреплялись вложениями с вредоносными программами, имели качественную HTML-вёрстку, а также часто содержали ссылки, которые сокращались через специальные сервисы и перенаправляли на вредоносные ресурсы. Эффективность на данном этапе выросла до 10%, так как обнаружить подделку стало проблематичнее.

Реальный случай: В 2010-х годах прокатилась массовая волна фишинговых писем от имени популярных сервисов, например, DHL. Письмо с темой «Ваша посылка ожидает получения» выглядело идеально: фирменные шрифты, логотипы, корректная вёрстка. В письме сообщалось, что для получения заказа не-

обходимо скачать и распечатать «накладную» во вложении. Этим вложением был файл TTH_Nº12345.exe, который на самом деле являлся трояном-кейлоггером. Также имел место всплеск фишинговых писем от имени Netflix с угрозой блокировки аккаунта и ссылкой на идеально скопированную страницу входа, которая похищала учётные данные.

3. Целевой фишинг

К этому этапу атаки стали носить точечный характер. Жертва заранее изучается через открытые источники, например, соцсети, а также используя слитые данные, утечки или купленную информацию. Целью является собрать все возможные личные данные — имя, место работы, контакты, даже круг общения [2].

Таким образом, электронное письмо или сообщение в мессенджер формируется для конкретного адресата, используя информацию о нём.

Речь в данном случае идёт о похищении значительных сумм или интеллектуальной собственности. Успешность достигает 35%.

Целевой фишинг имеет несколько специализированных разновидностей.

Spear Phishing (копьевой фишинг) — стандартный и широко используемый метод целевого фишинга. Атака нацелена на конкретного сотрудника внутри организации. Примером является сообщение бухгалтеру от «руководителя компании» с указанием срочно перевести деньги на мошеннический счёт.

Реальный случай: Бухгалтер компании получает письмо от имени финансового директора. Текст звучит правдоподобно: «Здравствуйте, [Имя бухгалтера]. Я на совещании, срочно нужно провести платёж по договору №45/ИП от сегодняшнего числа. Все детали во вложении. Связь плохая, пишите только на почту». Во вложении — инфицированный документ или ссылка на фальшивую страницу корпоративного портала.

Whaling (фишинг на топ-менеджмент) — по сути является копьевым фишингом, отличие в том, что целью являются чиновники высшего звена, директорат и другие высокопоставленные лица. Изучение жертвы проходит более тщательно, легенда формируется точнее и имитирует, например, судебные разбирательства или предложения от партнёров по бизнесу.

Реальный случай: В 2016 году киберпреступники, выдав себя за руководителя дочерней компании, с помощью серии фишинговых писем убедили CEO австрийского производителя авиационных компонентов FACC перечислить 50 миллионов евро на мошеннический счёт.

Smishing (SMS-фишинг) — данный метод может быть как обособленным, так и являться частью мошеннической схемы. Каналом связи в данном случае выступает служба коротких сообщений, текст которых содержит уведомление о выигрыше, курьерской доставке, блокировке карты и, конечно же, подозрительную ссылку.

Реальный случай: Сообщение: «Банк «XXX». По подозрению в мошенничестве ваша карта заблокирована. Для разбло-

кировки перейдите по ссылке: bank-xxx.ru/confirm». Ссылка вела на фишинговый сайт, запрашивающий все данные карты, включая CVV и одноразовые коды.

Vishing (голосовой фишинг) — атака, осуществляемая по телефону либо в мессенджерах. Мошенник, используя собранные о жертве данные, звонит ей под видом сотрудника IT-отдела, службы безопасности банка или техподдержки сервиса. Социальная инженерия и психологическое давление помогают выманить конфиденциальные данные, пароли или разрешить удалённый доступ к компьютеру.

Реальный случай: Звонок на номер сотрудника: «Здравствуйте, это техподдержка Microsoft. На вашем компьютере зафиксирована критическая уязвимость. Для её устранения нам потребуется удалённый доступ. Откройте программу AnyDesk и сообщите нам код». Далее под предлогом «защиты» мошенники похищали конфиденциальные данные или устанавливали шпионское ПО.

4. Высокотехнологичный фишинг

Современный фишинг использует передовые IT-технологии, такие как машинное обучение и генеративные AI. К сожалению, это значительно повышает его успешность. Автоматизация сбора и сортировки информации делает целевой фишинг массовым, что влияет на частоту атак.

Ключевые технологии и их применение

Тексты. Нейросети (например, ChatGPT, Gemini) применяются для создания орфографически и стилистически корректных сообщений на любом языке. Отсутствие явных ошибок позволяет обходить спам-фильтры и усложняет обнаружение пользователями. ИИ может написать текст на любую тематику, от официального до дружеского обращения.

Реальный случай: Мошенники используют ИИ для генерации персональных писем жертвам, найденным на LinkedIn, «Хабре» и других ресурсах. Вместо шаблонного «Уважаемый пользователь», письмо начинается так: «Здравствуйте, [Имя]. Прочитал вашу статью о кибербезопасности на Хабре — очень впечатляюще. У меня есть деловое предложение, ознакомиться можно здесь: [фишинговая ссылка, маскирующаяся под DocSend]». Отсутствие ошибок и персонализация обходят фильтры и вызывают доверие.

Deepfake (глубокие фейки) — самый опасный инструмент высокотехнологичного фишинга.

Используя технологии синтеза голоса по образцу голоса (например, на основе короткого аудиофрагмента публичного выступления или видео в социальной сети), хакеры создают поддельные голосовые сообщения или совершают телефонные звонки голосом, неотличимым от голоса настоящего человека.

Технология deepfake позволяет в режиме реального времени подменять лицо и голос человека на видео. Мошенник может организовать видеоконференцию, где на экране будет цифровой двойник генерального директора, отдающего приказ финансовому директору. Такие атаки обладают максимальной разрушительной силой, поскольку преодолевают последний барьер недоверия — визуальную верификацию.

Реальный случай (голосовой глубокий фейк): В 2019 году CEO британской энергетической компании получил телефонный звонок от своего «босса» — главы немецкой материнской компании. Голос с характерным немецким акцентом приказал срочно перевести 220 тысяч евро на счёт венгерского поставщика. Перевод был совершён немедленно, так как голос был абсолютно идентичен настоящему.

Реальный случай (видео глубокий фейк): В 2021 году мошенники использовали видео с глубокой подделкой лица и голоса директора инвестиционной компании, чтобы организовать фиктивную видеоконференцию с сотрудниками и юристами и санкционировать незаконную финансовую операцию.

Обсуждение

Представленная классификация демонстрирует, что эволюция фишинга происходит в тесном контакте технологий и человеческой психологии. Это определяет смену вектора противодействия угрозам с программно-аппаратных методов на комплексные подходы, ориентированные на человека.

На заре фишинга противодействие было в первую очередь техническим и фильтрующим. Почтовые фильтры отсеивали массовый спам по формальным признакам. Однако по мере того, как фишинг становился более целевым и изощрённым, одних лишь технических барьеров стало недостаточно. Мошенники начали использовать социальную инженерию, обходя стандартные защиты за счёт доверия к личности отправителя или релевантности содержимого. Это привело к смещению фокуса на человеческий фактор: повсеместному внедрению тренингов по киберграмотности, моделированию фишинговых атак для обучения сотрудников и разработке строгих организационных процедур (например, обязательной устной проверки для финансовых транзакций).

В настоящее время, с наступлением эры высокотехнологичного фишинга с использованием искусственного интеллекта и глубоких фейков, мы наблюдаем синтез этих двух подходов. Технологии снова выходят на первый план, но уже на качественно новом уровне. Для противодействия ИИ-генерации контента и голосовых подделок требуются столь же продвинутые средства защиты. Ожидается, что это повлечёт за собой повсеместное внедрение криптографических методов аутентификации, основанных на принципах «нулевого доверия», и усиление роли биометрических верификационных протоколов, которые сложнее скомпрометировать дистанционно [3]. Таким образом, будущее противодействия фишингу лежит в области гибридных моделей, где передовые технологии защиты усиливают бдительность человека, а осведомлённый пользователь становится последним и самым важным рубежом обороны.

Таблица 1.
Классификация эволюции фишинговых атак

	Ключевые характеристики	Примеры	Методы противодействия
1. Примитивный массовый фишинг (1990-е – ~2005)	Широкие нецелевые рассылки, низкое качество, лёгкое обнаружение	Письма от «банка» с просьбой подтвердить данные	Базовые фильтры спама, обучение пользователей распознаванию очевидных признаков (орфографические ошибки, подозрительные адреса отправителей), проверка URL перед кликом
2. Технологический фишинг (~2005 – ~2015)	Использование уязвимостей, трояны, улучшенный дизайн	Внедрение кейлоггеров, фишинговые сайты-клоны	Антивирусное ПО, фаерволы, регулярное обновление ПО для закрытия уязвимостей, двухфакторная аутентификация (2FA), использование безопасных браузеров с проверкой сертификатов
3. Целевой фишинг (~2010 – по н.в.)	Точечные атаки на конкретных людей/компаний, социальная инженерия	Целевые письма от имени коллеги или руководства	Повышенная киберграмотность, тренировки по распознаванию фишинга, строгие процедуры проверки запросов на перевод средств/данных, сегментация сетей для ограничения доступа
4. Высокотехнологичный фишинг (~2018 – по н.в.)	Использование AI, глубоких фейков, автоматизации	Deepfake-звонки, AI-генерация писем	Поведенческий анализ и AI-детекция аномалий, биометрическая и многофакторная аутентификация (MFA), использование кодовых слов/фраз для подтверждения критических запросов, продвинутые системы мониторинга трафика и почтовых угроз

Заключение

Развитие фишинга двигалось от неточных, массовых рассылок с массой ошибок и вызывающими заголовками к высокотехнологичным атакам на конкретного человека. Ранее методы противодействия заключались в технологической составляющей, такой как спам-фильтры, антивирусы. Теперь основой интернет-безопасности является человеческий фактор.

Ни одно даже самое передовое и актуальное техническое решение не может гарантировать 100% защиты от злоумышленников. Поэтому к методам современной защиты следует отнести:

- регулярное тестирование и обучение сотрудников основам информационной безопасности;
- внедрение строгих процедур для подтверждения финансовых транзакций (использование кодовых слов, многократная проверка по разным каналам связи);
- технологические решения: DMARC, DKIM, SPF для проверки почты, системы мониторинга угроз.

Фишинг из грубого инструмента мошенников превратился в сложное оружие киберпреступников. И единственный адекватный

ответ на эту угрозу — сочетание технологий, процедур и, что самое главное, осведомленности и бдительности каждого человека. ■

Список литературы:

- [1] Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения. — Baikal Research Journal, 2022. — №2. — С. 36-42.
- [2] Фишинг: как распознать и не стать жертвой мошенников [Электронный ресурс] URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips> (дата обращения: сентябрь 2025).
- [3] Что такое фишинг? [Электронный ресурс] URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-phishing> (дата обращения: сентябрь 2025).

Об авторе

Гавриченко Николай Егорович, координатор разработки продуктов Фонда развития сетевых технологий «ИнДата», ассистент кафедры интеллектуальных систем и теплофизики ИИР НГУ.