

ФИШИНГ КАК МЕТОД КИБЕРМОШЕННИЧЕСТВА

Фишинг — это метод кибермошенничества, используемый преступниками для похищения личной информации пользователей. Обычно реализуется через электронные письма, СМС или сообщения в социальных сетях, имитирующие легитимные запросы от надежных организаций (банков, соцсетей, госучреждений).

Цель — заставить жертву добровольно раскрыть конфиденциальные данные, перейдя по подложной ссылке на сайт-клон или заполнив форму с личными данными (пароль, реквизиты банковских карт). Для повышения доверия используются логотипы и фирменные стили настоящих компаний.

Примеры фишинга:

1. Поддельные письма банков *Пример:* Сообщение якобы от банка с просьбой подтвердить данные карты («Ваш аккаунт заблокирован») с требованием пройти аутентификацию на сайте-клоне.
2. Социальные сети и сервисы *Пример:* Фальшивая ссылка на обновление профиля соцсети, ввод данных аккаунта, номер телефона или подтверждение регистрации новым способом.
3. Электронная почта *Пример:* Подделанные уведомления от известных сервисов вроде Google, Amazon или AliExpress с предложением срочно обновить профиль или оплатить заказ.

Как распознать фишинг?

Проверяйте адрес отправителя.

Часто подделываются адреса электронной почты крупных компаний.

Обращайте внимание на орфографические ошибки и небрежность оформления.

Никогда не переходите по подозрительным ссылкам сразу.

Лучше вручную зайдите на сайт сервиса.

Будьте осторожны с вложениями и файлами. Они часто содержат вредоносные программы.

Полезные советы:

Используйте двухфакторную аутентификацию везде, где возможно. Это значительно снизит риск кражи данных даже при попадании злоумышленникам вашего пароля.

Примеры популярных схем фишинга:

- Банковский фишинг: письма с сообщением о проблемах с картой или аккаунтом, призывающие немедленно проверить данные на поддельном ресурсе.
- Фишинг через социальные сети: фейковые страницы входа, уведомляющие о взломе или срочной проверке учетной записи.
- Коронавирусный фишинг: использование пандемии COVID-19 для распространения ссылок на поддельные анкеты вакцинации или проверки состояния здоровья.

Для защиты важно проверять подлинность ресурсов перед введением данных, избегать перехода по сомнительным ссылкам и регулярно обновлять антивирусы и браузеры.

Фишинг — это распространенный способ онлайн-мошенничества, цель которого — похитить личную информацию пользователей, такую как пароли, банковские реквизиты и прочие важные данные. Преступники используют методы психологического воздействия, маскируя себя под известные бренды, банки или государственные учреждения.

Основные типы фишинга:

- Массовая рассылка: Электронные письма отправляются миллионам пользователей одновременно, пытаясь привлечь внимание с помощью общих формулировок ("Проблемы с вашим счетом").
- Целевой фишинг: Направлен на конкретных лиц или организации, используется персонализированная информация, повышается доверие жертвы.
- SMS-фишинг: Жертва получает сообщение с текстом типа "Вы выиграли приз, подтвердите свои данные".

Статистика:

По данным исследований последних лет, количество атак фишинга ежегодно растет примерно на 15%. Чаще всего жертвами становятся обычные пользователи и небольшие предприятия, хотя крупные корпорации также подвергаются риску. Защита от фишинга включает комплекс мер предосторожности и внимательного отношения к сетевым взаимодействиям.

Вот основные рекомендации:

Способы защиты от фишинга:

1. Проверяйте источник сообщения
 - Убедитесь, что электронное письмо действительно пришло от доверенного отправителя. Проверьте название домена в адресе почтового сервера.
2. Будьте бдительны с гиперссылками
 - Никогда не кликайте на незнакомые ссылки, особенно в письмах или сообщениях. Если сомневаетесь, скопируйте ссылку и вставьте её в браузер самостоятельно, предварительно проверив правильность написания адреса.
3. Двухфакторная аутентификация (2FA)
 - Включите двухэтапную проверку для важных аккаунтов (электронная почта, финансовые услуги, социальные сети). Даже если ваш пароль украден, дополнительная проверка затрудняет доступ злоумышленнику.
4. Регулярно обновляйте программное обеспечение
 - Используйте современные версии операционных систем, браузеров и приложений. Обновления включают исправления уязвимостей, используемых фишерами.
5. Используйте антивирусные решения
 - Установите надёжное антивирусное ПО, которое способно обнаруживать и предупреждать о потенциально опасных сайтах и приложениях.
6. Остерегайтесь вложений
 - Не открывайте вложения от неизвестных отправителей, особенно файлы .exe, .zip или .rar. Такие архивы могут содержать вирусы или шпионские программы.
7. Обучайте сотрудников и близких

- Повышение осведомлённости среди коллег и членов семьи помогает снизить риски попадания в ловушку фишинга. Регулярные инструктажи и обучение предотвращают многие инциденты.

8. Пользуйтесь официальными контактами

- При получении неожиданных запросов от финансовых учреждений или государственных органов обратитесь напрямую к официальным источникам (например, позвоните в службу поддержки).

Следуя этим рекомендациям, вы существенно повысите уровень своей цифровой безопасности и защитите свою персональную информацию от несанкционированного доступа.

Зайцев Олег Николаевич

Доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Шахраманьян Михаил Андраникович

Профессор кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ