StopPhish

ТЕХНИЧЕСКИЙ ЧЕК-ЛИСТ

Защита от фишинга и социальной инженерии

Проверьте, корректно ли ваши системы обрабатывают методы визуальной и технической маскировки — ссылок, вложений и содержимого писем.

СПОСОБЫ ПРИМЕНЕНИЯ ЧЕК-ЛИСТА

01

Убедитесь, что системы защиты сработают при различных методах маскировки ссылок, вложений и текста.

02

Стройте учебные материалы для повышения осведомлённости сотрудников на основе пунктов чек-листа.

03

Корректируйте внутренние регламенты: разным группам пользователей — разные правила доступа.

> Выбирайте тактику фильтрации: **«всё запрещено, отдельное разрешено»** или **«всё разрешено, отдельное запрещено»**.

ЗАЩИТА ОТ ФИШИНГОВЫХ ССЫЛОК

- **Ссылки с символом @** — браузер воспринимает всё до @ как учётные данные, а не как домен:

```
yandex.ru:news-1421@yanedx.ru
```

- **Слеш в Unicode (U+0B75)** — чаще всего комбинируется с символом @ в ссылке:

```
https://www.ya.ru৵news:in@yanedx.ru
```

- **Обфускация IP через urlencode** — IP-адрес скрыт за нечитаемой строкой. Например, IP mail.ru может выглядеть так:

```
https://0xd9.0x45.0x8b.0xca/company.ru
https://0331.0105.0213.0312/google.ru
https://3645213642/ya.ru + комбинации способов маскировки
```

- **QR-коды** в теле письма.
- **Текстовые ссылки в виде картинок** в теле письма.
- **Некорректный синтаксис в href:**

```
http:\\bank.ru
http:/.bank.ru
//bank.ru
```

Домен нулевого уровня не относится к некорректному синтаксису, но может небезопасно обрабатываться ИТ-системами: `reg.ru./vps` работает так же, как `reg.ru/vps`.

- **Ссылки в документах во вложении.**
- **Официальные домены в других доменных зонах.**
- **Очень длинные ссылки** — применяются, например, с символом «@»:

```
http://yandex.ru.668-sdfsadf-ajay.com-123788125-ajayasjjba.com-sdmasdlhuaoqw@zlo.ru/sdfsadf-ajayasjjba.com/sdmasd.ru-lhuaoqw#sdfsadf-ajayasjjbasdmasdlhuaoqw?sdfsadf-ajay-asjjba123955w&sdfsadfajay-asjjbasdmasdlhuaoqw
```

- **IP вместо домена:**

```
https://94.100.180.201
```

- **Редиректы:**
  - видимые: `https://ya.ru/?r=bit.ly/12365`
  - скрытые: `https://ya.ru/?r=12365`
- **Неактивные ссылки** — не работают при клике, побуждают скопировать и вставить в браузер (например: `yadnex.ru`).
- **Похожие на официальные сайты:**
  - добавление букв — `yanedex.ru`
  - бит-сквоттинг — `yaendex.ru`
  - гомоглифы, пропуск символов — `yandx.ru`
  - поддомен — `y.andex.ru`
  - подмена гласных — `yondex.ru`

Утилита `Dnstwist` позволяет сгенерировать похожие домены на основе вашего официального и добавить их в блок-лист.

- **Ссылки в поддоменах:**

```
https://yandex.ru.yanexd.ru
```

- **URL в открытом виде, а href отличается** — в письме видна ссылка `https://ya.ru`, а ведёт она на `https://yo.ru`. Не путайте со случаями, когда ссылка прописана как обычный текст — иначе будет много ложных срабатываний.

- **Кириллические домены** — используются совместно с другими методами маскировки. Например, домен `кто.рф` в punycode: `xn--j1ail.xn--p1ai`. Можно применять в редиректах или через urlencode:

```
http://%D0%BA%D1%82%D0%BE.%D1%80%D1%84
```

ЗАЩИТА ОТ ВРЕДОНОСНЫХ ВЛОЖЕНИЙ

Решите, какие расширения блокировать в 100% случаев, а для каких сделать исключения для отдельных групп пользователей (например, если в вашей работе используются `.000`, `.001` и т.д.).

ОПАСНЫЕ РАСШИРЕНИЯ

`accdb` `ade` `adp` `apk` `appx` `appxbundle` `bat` `cab` `chm` `cmd` `com` `cpl` `dll` `dmg` `exe` `hta` `ins` `isp` `iso` `img` `jar` `js` `jse` `lib` `library-ms` `lnk` `mde` `msc` `msi` `msix` `msixbundle` `msp` `mst` `nsh` `pif` `ps1` `scr` `sct` `searchconnector-ms` `shb` `sys` `vb` `vbe` `vbs` `vsdm` `vssm` `vxd` `wsc` `wsf` `wsh`

ВОЗМОЖНЫЕ К ЗАПРЕТУ — ИСПОЛЬЗУЮТСЯ В ФИШИНГЕ

`html` `htm` `xhtml` `mhtml`

- Файлы с расширениями из списка выше, включая сжатые (GZ, BZ2) и помещённые в архив (ZIP, TGZ).

- Архивы, защищённые паролем.

- Архивы, содержащие защищённые паролем архивы.

- Документы с макросами.
- Документы с макросами в архиве.

АУТЕНТИФИКАЦИЯ EMAIL-ОТПРАВИТЕЛЯ

Убедитесь, что у вас корректно настроены все три протокола защиты от поддельных отправителей.

DKIM

Цифровая подпись письма — подтверждает, что содержимое не изменялось в пути.

SPF

Список доверенных серверов-отправителей для вашего домена.

DMARC

Политика обработки писем, не прошедших проверку DKIM или SPF.

ЗАЩИТА ПО СОДЕРЖИМОМУ ПИСЬМА

> *Методы маскировки из этого раздела чаще применяются при массовых атаках или рассылке спама.*

- **Цифры вместо букв:**

```
0повещение, Доб́рый
```

- **Латинские буквы вместо русских** (визуально неотличимы):

```
Добрый день
```

- **Символы Unicode вперемешку с обычным алфавитом:**

```
Ответ на письмо
```

- **Разбавление спецсимволами:**

```
Доб_рый д ень
```

Предлагайте свои рекомендации — мы дополним список.
С уважением, команда StopPhish

StopPhish.ru