Ключевые правила профилактики фишинга

Включают меры по защите от подозрительных сообщений, настройки браузера, созданию надёжных паролей и использованию антивирусного ПО. Важно быть осведомлённым о фишинговых методах и соблюдать правила безопасности в интернете

Электронная почта

- **Не отвечать на подозрительные сообщения** и не переходить по ссылкам, которые не запрашивались. Мошенники могут подделать адрес отправителя, чтобы сделать письмо более правдоподобным. Если есть сомнения в подлинности письма, обратиться в службу поддержки компании и уточнить информацию.
- **Не открывать вложения** из писем от незнакомцев. Фишинговые письма могут содержать неожиданные файлы: документы, архивы или программы (например, .doc, .zip, .exe). Эти вложения часто заражены вирусом. **Настроить фильтры спама** в электронной почте и мессенджерах — это поможет уменьшить количество фишинговых сообщений.
- **Включить двухфакторную аутентификацию** для сетевых учётных записей — это добавляет дополнительный уровень безопасности, требуя второго шага (например, кода, отправленного на телефон) перед входом.

Интернет-браузер

- **Переходить только на безопасные сайты** — защищённые соединения между браузером и сайтами шифруют данные, в противном случае мошенники могут перехватить информацию. Например, в адресной строке сайта должен быть значок замка (HTTPS).
- **Проверять URL-адрес** — фишинговые сайты зачастую визуально копируют реальные сайты популярных сервисов, но адрес в браузере выдаёт подделку. Нужно навести курсор на ссылку, не кликая, чтобы увидеть реальный адрес. Если адрес отличается от официального или выглядит странно, не переходить. **Настроить защищённое соединение** в настройках браузера, например, в Chrome — «Всегда использовать безопасные соединения», в Яндекс Браузере — «Автоматически открывать сайты по протоколу HTTPS».
- **Отключить синхронизацию паролей** и автозаполнение, если браузер автоматически сохраняет пароли. **Пароли**
- **Создавать сложные пароли** — они включают не менее 10 символов (буквы и цифры), большие и маленькие буквы, знаки препинания и символы. Не стоит вписывать в пароль личные данные — например, дату рождения или фамилию.
- **Не использовать один пароль** для разных сайтов — если злоумышленники взломают одну учётную запись, то получат доступ и к другим.

- **Использовать менеджеры паролей** — они помогают генерировать сложные случайные пароли и хранить их.
- **Регулярно обновлять пароли** — особенно после утечки данных или подозрительных активностей.
- **Включить двухфакторную аутентификацию** — это добавит дополнительный уровень защиты, требуя подтверждения входа с помощью дополнительного кода, который отправляется на телефон или другую аутентификацию.

Антивирус

- **Использовать антивирус с функцией защиты от веб-угроз** — это помогает блокировать подозрительные веб-сайты, которые могут быть использованы злоумышленниками для кражи данных. Антивирусное ПО может предупреждать пользователей о потенциальной угрозе, прежде чем они смогут перейти на опасный сайт.
- **Регулярно обновлять антивирус** — это поможет защитить от новых угроз.
- **Использовать многофункциональное антивирусное решение** — оно включает не только защиту от вирусов, но и инструменты для защиты от фишинга.

Важно понимать, что использование антивирусного ПО — лишь один из элементов комплексной стратегии безопасности — не менее значимыми являются осведомлённость пользователей о фишинговых методах и соблюдение простых правил безопасности в интернете.