SEARCHINFORM
INFORMATION SECURITY

3 шага
для распознавания мошеннического сайта

Используйте чек-лист, чтобы обучить сотрудников базовым правилам киберграмотности.

Фишинговые сайты –
по-прежнему популярный инструмент мошенников, используемый в самых разных схемах.
Угроза актуальна как для обычных юзеров, так и для бизнеса – через невнимательных сотрудников злоумышленники крадут данные компаний, заражают вирусами корпоративную инфраструктуру и др. По данным ежегодного исследования «СёрчИнформ», в 2022 году 11% российских компаний столкнулись с внешней атакой через сотрудников.

1 Каким образом вы получили ссылку на сайт?

Чаще всего ссылки на мошеннические сайты приходят по почте. Поэтому обращайте внимание на письма. **Базовые признаки письма**, которое ведет на мошеннический сайт: побуждение к немедленному действию (смена пароля/логина, срочная оплата штрафа и др.), наличие гиперссылки в письме.

Мошенники также распространяют ссылки на фишинговые сайты через мессенджеры, QR-коды и рекламу (социальные сети/поисковая выдача).

2 Какой адрес у сайта?

Если ссылка на сайт вызывает подозрение, то проверьте:

- **адрес/название домена.** Мошенники часто используют **тайпсквоттинг** – похожее написание бренда, в котором вместо буквы может использоваться цифра, опечатки, другая доменная зона (.com вместо .ru, например) и т.п. Дополнительные признаки фишингового сайта разобрали в подборной статье по ссылке.
- **возраст сайта и владельца.** Для этого можно использовать любой сервис Whois. Мошенники используют домены как расходный материал, срок их «жизни» может составлять от нескольких часов до нескольких дней. «Свежий» адрес, зарегистрированный на частное лицо – повод для дополнительных подозрений.

3 Какое содержимое сайта?

- **тематика:** некоторые темы, как правило, мошеннические сами по себе, например, 100%-ный возврат денег, похищенных нечестным брокером.
- **текст:** слишком многообещающий. Встречаются ошибки. Используются фрагменты, которые можно через интернет-поиск найти на других аналогичных сайтах.
- **видео:** для убедительности встроены видео «клиентов», которые однообразно описывают свой опыт только в положительном ключе.
- **изображения:** используются краденные картинки. Если на этом этапе сайт вызывает у вас подозрения, то можно проверить, где еще используются фотографии, например, экспертов/сотрудников. Проверить это можно с помощью поиска по изображениям.
- **заглушки и имитация функционала:** задача сайта сводится к заполнению формы-заявки, остальные разделы сайта могут не работать или перебрасывать пользователя на главную страницу.