ФИШИНГОВЫЕ ПИСЬМА

SCS SBER CYBER SECURITY

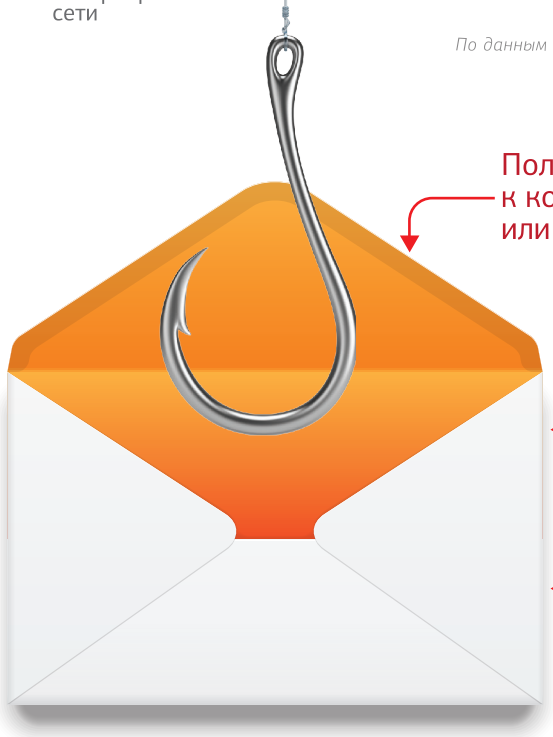
в 98% случаев
вредоносные программы скрываются во вложениях писем, и только в 2% — в ссылках

одного СОТРУДНИКА,
случайно запустившего вредоносное ПО, достаточно, чтобы мошенники получили доступ ко всей корпоративной сети

в 54% случаев
люди сами устанавливают вредоносные приложения или передают данные мошенникам

По данным ФинЦЕРТ Банка России, Group IB и Trend Micro

ЦЕЛИ МОШЕННИКОВ



- Получить доступ к компьютеру или корпоративной сети
- Заставить перейти на мошеннический сайт
- Украсть конфиденциальную информацию
- Выудить персональные данные
- Получить доступ к банковской карте

ЧТО ПИШУТ В ФИШИНГОВЫХ ПИСЬМАХ

- Получите выигрыш, призовой абонемент, подарок, бонус
- Подтвердите аккаунт на знакомом ресурсе
- Срочно подтвердите транзакцию
- Ваш аккаунт заблокирован, нужны ваши данные
- Произошла утечка данных
- Получите платежный документ и обналичьте деньги
- Вам выплаты от государства
- Оплатите налог (вот чек!)

БУДЬТЕ БДИТЕЛЬНЫ!

Используйте корпоративную технику для работы с конфиденциальными материалами

Установите антивирус
Он поможет распознавать фишинговые письма

Удаляйте письма с сомнительными ссылками или подозрительными вложениями, особенно в форматах EXE, HTML, JAR, PIF, HTA, MSI

Сомневайтесь в письмах с сообщениями о бонусах, премиях, выигрышах и опросах за вознаграждение

Проверяйте адреса, с которых приходят письма. Даже если кажется, что они от надежного адресанта

Будьте бдительны
Мошенники часто пишут на корпоративные адреса

Будьте внимательны в праздники
Мошенники могут рассылать письма, стилизуя их под поздравления