Министерство цифрового развития и связи
Оренбургской области

digital.orb.ru

ПРАВИЛА ПРОТИВОДЕЙСТВИЯ ПОПЫТКАМ ВЗЛОМА В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ, А ТАКЖЕ ФИШИНГОВЫМ АТАКАМ

Оренбургская область
2024 г.

Фишинг (phishing) – разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником.

Фишинг – один из популярных видов мошенничества в интернете

Мошенники выманивают у пользователей конфиденциальную информацию: от логинов и паролей к почтовым ящикам до информации о банковских картах. При этом могут использоваться разные способы: электронные письма, ссылки в мессенджерах и SMS, поддельные страницы популярных онлайн-сервисов.

Электронная почта остается главной лазейкой для фишеров

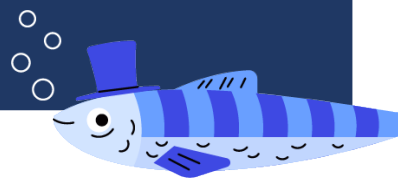
Как сообщается на сайте securitylad.ru, эксперты Positive Technologies проанализировали фишинговые атаки на организации в 2022-2023 годах и выявили основные тенденции и угрозы.

85%
атак
для получения данных

26%
атак
финансовые выгоды

Украденная информация может быть продана в дарквебе или использована для шпионажа. Среди киберпреступников особенно активны хактивисты, которые стремятся нанести ущерб своим жертвам из политических или идеологических мотивов.

В исследовании говорится, что «фишинг как услуга» стал обычной практикой, эксперты прогнозировали такое распространение киберуслуг несколько лет назад. Сегодня эту бизнес-модель используют как профессиональные APT-группировки и опытные злоумышленники-одиночки, так и новички, не обладающие специальными знаниями и навыками.



Электронная почта остается главной лазейкой для фишеров

Большинство фишинговых атак осуществляется через:

Часто они выдают себя за руководителей или сотрудников организаций, для чего им достаточно знать их имена и фотографии*. Самой популярной уловкой является выдача себя за контрагентов (26% атак), когда фишеры присылают поддельные документы, связанные с взаимодействием с подрядчиками.

Жертвы фишинга

44%

атак с отраслевой направленностью

госучреждения

19%

оборонные предприятия

14%

организации в сфере науки и образования

Виды фишинга

Социальная инженерия

Фишинговые ссылки

Фишинговые сайты

Фишинговые приложения

Ловля «на живца»

Претекстинг

Уэйлинг

1.Социальная инженерия

Это метод фишинга без использования специальных технических средств. Мошенник никого не взламывает, не подсаживает вирусы, не перехватывает трафик. Все данные человек выдает сам — под действием обмана, угроз и манипуляций. Когда аферисты притворяются сотрудниками полиции, Центробанка и ФСБ — это как раз социальная инженерия.

2.Фишинговые ссылки

Задача мошенника — убедить получателя письма или сообщения, что нужно перейти по присланной ссылке. Этот метод особенно популярен на досках объявлений вроде «Авито». Скажем, покупатель пишет продавцу, что уже оплатил товар и доставку и тому надо лишь получить свои деньги на сайте avito-dostavka-msk.ru, avito-deiiveri.ru или что-то в этом роде.

По ссылке откроется фишинговый сайт — почти точная копия настоящего. С одним отличием: все данные, которые вы там введете, попадут в руки мошенникам.

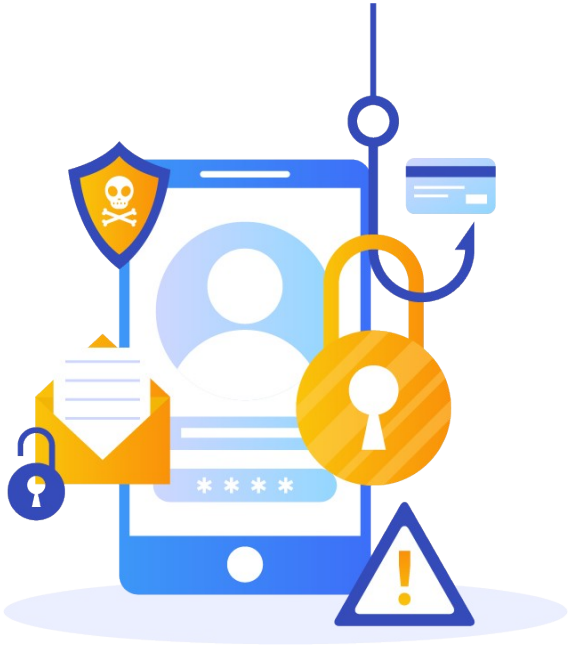
3.Фишинговые сайты

Когда в России стала популярна социальная сеть «Вконтакте», мошенники освоили такой прием. Они писали людям с незнакомого аккаунта что-то вроде «Ну ты вчера и зажег на вечеринке! Фотки просто стыдоба, зацени!» — и кидали фишинговую ссылку на сайт, который полностью копировал окно входа в социальную сеть, тем самым происходила кража учетной записи ВКонтакте

Часто мошенники копируют сайты крупных компаний, которые обещают поделиться доходами со всеми желающими. Например, фальшивый сайт «Газпрома», на котором всем гражданам России обещали по 8500 $ в месяц. Пострадавших были готовы принять другие мошенники — из «Азиатского фонда защиты инвесторов», который маскировался под настоящий фонд.

Только за первые два месяца 2023 года российские специалисты по безопасности обнаружили **5,2 тысячи** фишинговых сайтов — в три раза больше, чем за аналогичный период 2022. Из них Роскомнадзор заблокировал всего **10% подделок — 523 сайта.**

4.Фишинговые приложения

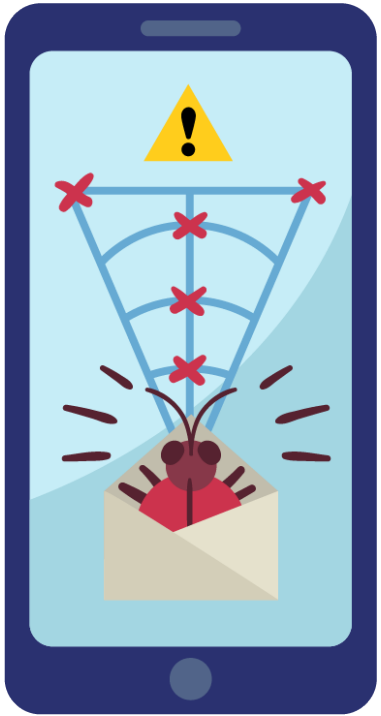


Подделки в магазинах приложений были чуть ли не с самого их открытия. Но после того как из Google Play и App Store удалили приложения крупных российских банков и компаний, подделок стало в разы больше: появились мошеннические копии RuStore и RuMarket, приложений Сбербанка и ВТБ.

Зачастую там просто показывают рекламу, а мошенники получают за это вознаграждение. Но некоторые приложения требуют предоставить им доступ к фотографиям или данным телефона. Хакеры сканируют устройство, находят чувствительные данные, а затем используют их для шантажа или взлома.

Это самый популярный метод фишинга. По данным компании Positive Technologies, на социальную инженерию в 2022 году пришлось 43% успешных атак на компании и 93% — на физлиц.

5.Ловля «на живца»



Хакер оставляет возле офиса флешку с надписью «Пароль от биткоин-кошелька» или диск «Зарплатная ведомость руководства». Расчет на то, что кто-то из сотрудников вставит носитель в свой компьютер, заразит его вирусом и тем самым предоставит хакеру доступ во внутреннюю сеть компании.

Учеными был проведен эксперимент, чтобы выяснить, насколько люди склонны использовать найденные устройства, — и разбросали по территории университета **297 флешек**. Когда кто-то подключал их к компьютеру с выходом в интернет, ученым приходило оповещение. В итоге оказалось, что сигнал подала почти **половина флешек**.

6.Претекстинг

Метод, когда мошенник сначала разыгрывает невинный спектакль, чтобы разогреть потенциальную жертву: например, проводит опрос про любимые музыкальные группы. А потом предлагает оставить данные банковской карты, чтобы получить вознаграждение. Или представляется службой технической поддержки работодателя, задает обычные вопросы, а потом просит логин и пароль от учетной записи, чтобы что-то обновить. Разводы с заполнением анкет и опросов тоже используют этот прием.

Как и большинство других мошеннических приемов, претекстинг нацелен не на взлом компьютера, а на использование уязвимостей нашей психики — чтобы сработал человеческий фактор. Ключевой момент в следующем рассказе нашего читателя — предварительная переписка с мошенником. Это и отличает претекстинг от обычного фишинга.

7.Уэйлинг

Некоторые мошенники вместо массовых атак предпочитают узкоспециализированные и хорошо подготовленные. Такие схемы называют whaling phishing или whaling attack, дословно — «охота на китов».

«Охотники на китов» тщательно изучают структуру компаний и пытаются понять, кому и от чьего имени можно написать, чтобы быстро и без подозрений украсть деньги или данные.

Как защититься от фишинга: 6 советов

Каждый раз мошенники пытаются придумывать все новые и более изощренные способы усыпить бдительность пользователей. Есть несколько способов, которые помогут предотвратить это.

1

Внимательно проверяйте электронные письма

2

Не теряйте бдительность в мессенджерах и социальных сетях

3

Перед вводом номера карты остановитесь!

4

Используйте разные пароли

5

Включите двухфакторную аутентификацию для защиты аккаунтов

6

Используйте надежную защиту

Создание пароля

- Надежные пароли по-прежнему являются простым, но верным способом защитить себя от мошенников.
- Не используйте один и тот же пароль для всех своих учетных записей.
- Рекомендуем также установить код-пароль, после которого над списком чатов будет появляться значок блокировки/разблокировки приложения.

Двухфакторная аутентификация

Для повышения степени защиты аккаунта в мессенджере рекомендуем вам установить двухэтапную проверку для получения доступа в свой аккаунт. Для этого следует также выбрать раздел «Конфиденциальность» в «Настройках» и переключить тумблер на «вкл» рядом с графой «Облачный пароль» . Далее вводим пароль, подсказку для пароля и электронную почту, куда придет проверочный код для завершения настройки двухфакторной авторизации.

Настройки → Конфиденциальность → Облачный пароль

Проверка скачиваемых файлов

- Всегда обращайте внимание на название расширения.
- Установите на устройство антивирус, который будет проверять все файлы на наличие угроз.
- В настройках мобильного устройства запретите установку из неизвестных источников.
- В настройках ПК укажите, что установка возможна только после получения разрешения.

Примеры фишинговых атак

HTTP://КРУТОЙРЮКЗАК.РФ

ВВЕДИТЕ ДАННЫЕ КАРТЫ

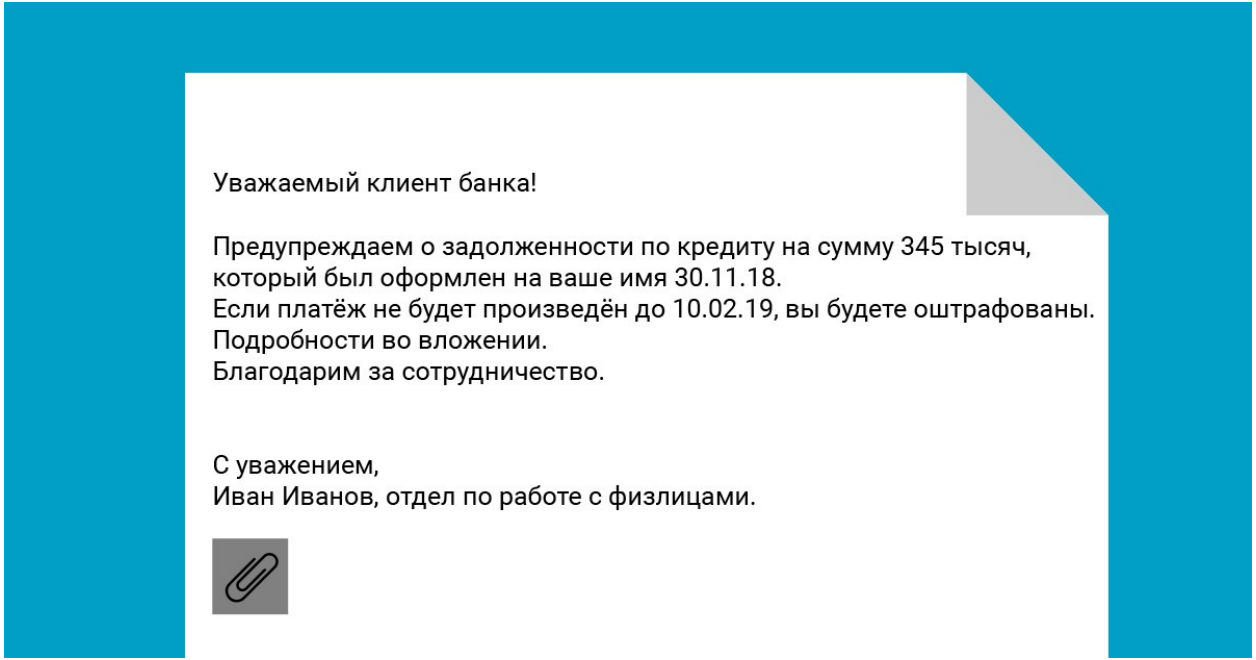
Вы покупаете рюкзак в интернет-магазине и переходите на страницу оплаты. Здесь всё в порядке? Можно платить?

Примеры фишинговых атак

Адрес вашего банка – berbank.ru. Выберите безопасную ссылку:
1.https://www.berbank.ru.action.ru
2.https://www-action.berbank.ru
3.https://berbank.ru/login?r.php=action.ru

Ваш друг в социальной сети пишет: «Зацени, что я нашел https://vk.cc/8WHTS9»
1.Перехожу по ссылке и ввожу то, что попросят на сайте. Друг плохого не посоветует.
2.Перейду по ссылке, и если у меня запросят пароль, уточню у друга, действительно ли он мне ее отправлял.

Вы получили такое письмо из банка. Откроете файл с подробностями?



Будьте бдительны и осторожны!