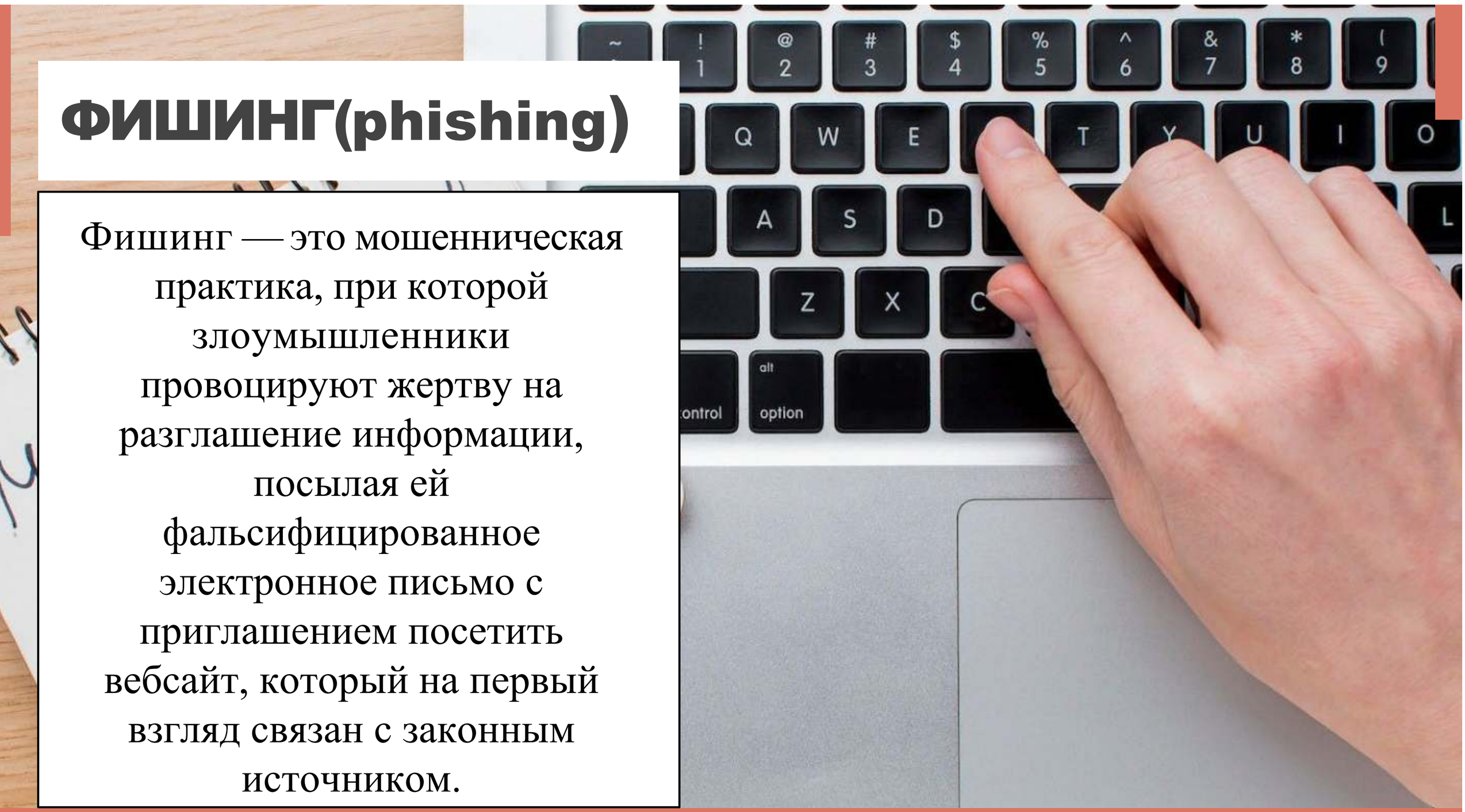
Методы противодействия попыткам взлома в социальных сетях и мессенджерах, а также фишинговым атакам

ФИШИНГ(phishing)

Фишинг — это мошенническая практика, при которой злоумышленники провоцируют жертву на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить вебсайт, 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 злоумышленникиодиночки, так и новички, не обладающие специальными знаниями и навыками.

Электронная почта остается главной лазейкой для фишеров

Большинство фишинговых атак осуществляется через:

89% – электронная почта
8% – мессенджеры
3% – СМС – сообщения

Часто они выдают себя за руководителей или сотрудников организаций, для чего им достаточно знать их имена и фотографии

Жертвы фишинга

44%

атак с отраслевой направленностью
госучреждения

19%

оборонные предприятия

14%

организации в сфере науки и образования

ВИДЫ ФИШИНГА

Существует несколько видов фишинга:

Социальная инженерия
Фишинговые ссылки
Фишинговые сайты
Фишинговые приложения
Ловля на живца
Претекстинг
Уэйлинг

1.Социальная инженерия

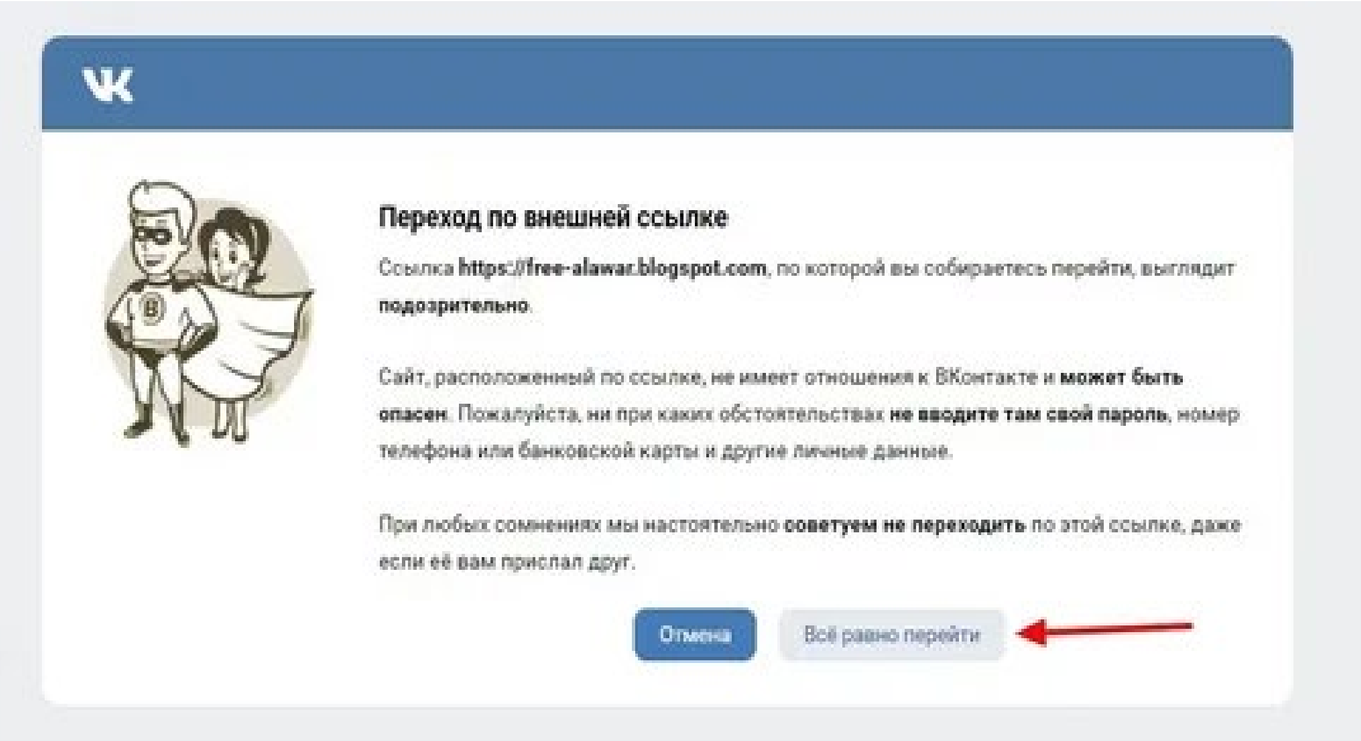
Это метод фишинга без использования специальных технических средств.

без вирусов **без взлома** **без перехвата трафика**

По данным компании Positive Technologies, на социальную инженерию в 2024 году пришлось около **43%** успешных атак на компании и **93%** — на физлиц.

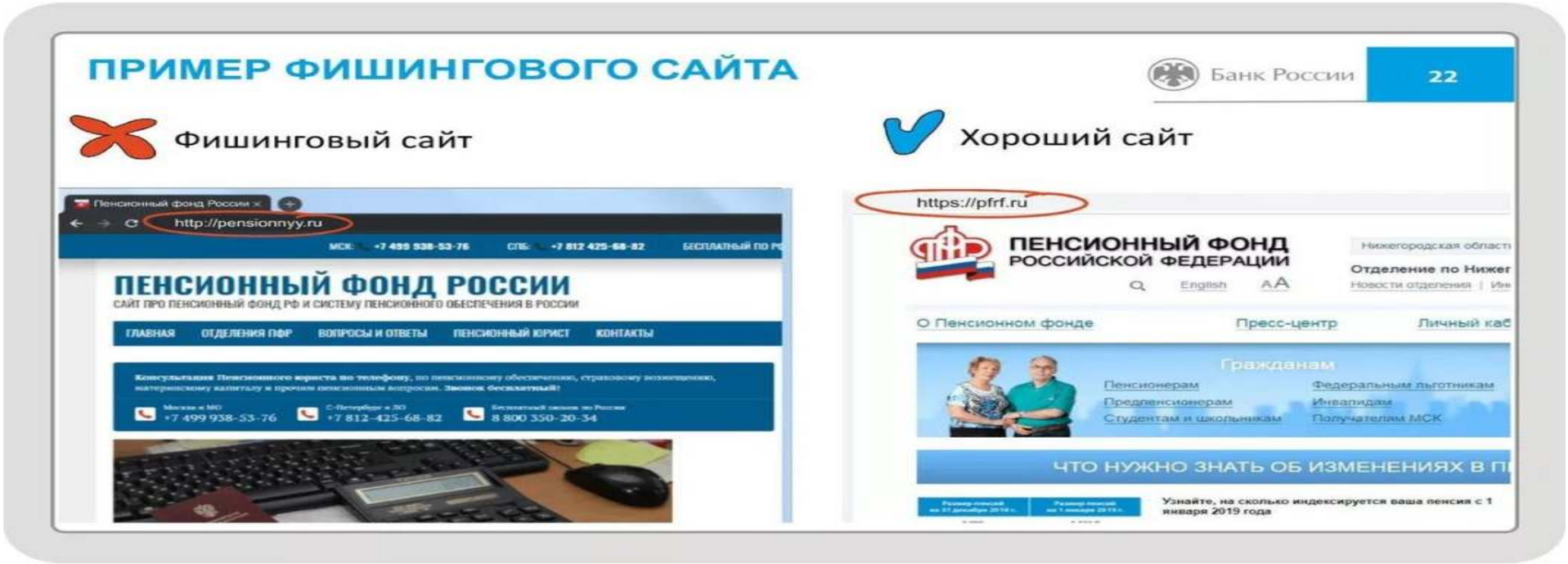
2.Фишинговые ссылки

Задача мошенника — убедить получателя письма или сообщения, что нужно перейти по присланной ссылке.



3.Фишинговые сайты

Часто мошенники копируют сайты крупных компаний, которые обещают поделиться доходами со всеми желающими.



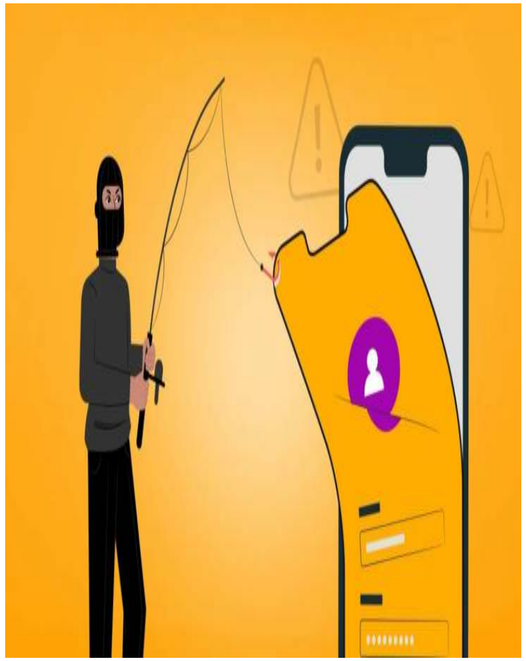
Только за первые два месяца 2024 года российские специалисты по безопасности обнаружили **5,2 тысячи** фишинговых сайтов — в три раза больше, чем за аналогичный период 2023. Из них Роскомнадзор заблокировал всего **10% подделок — 523 сайта**

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.

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

5.Ловля на живца



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

Был проведён 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 интнернет, приходило оповещение. В итоге оказалось, что сигнал подала почти **половина флешек**.

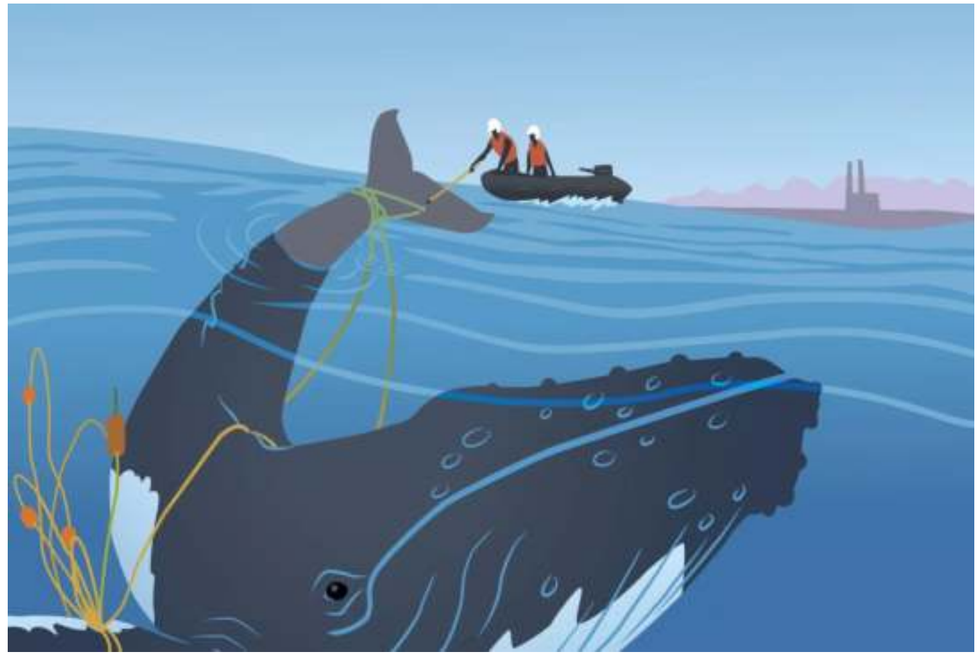
6.Претекстинг

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

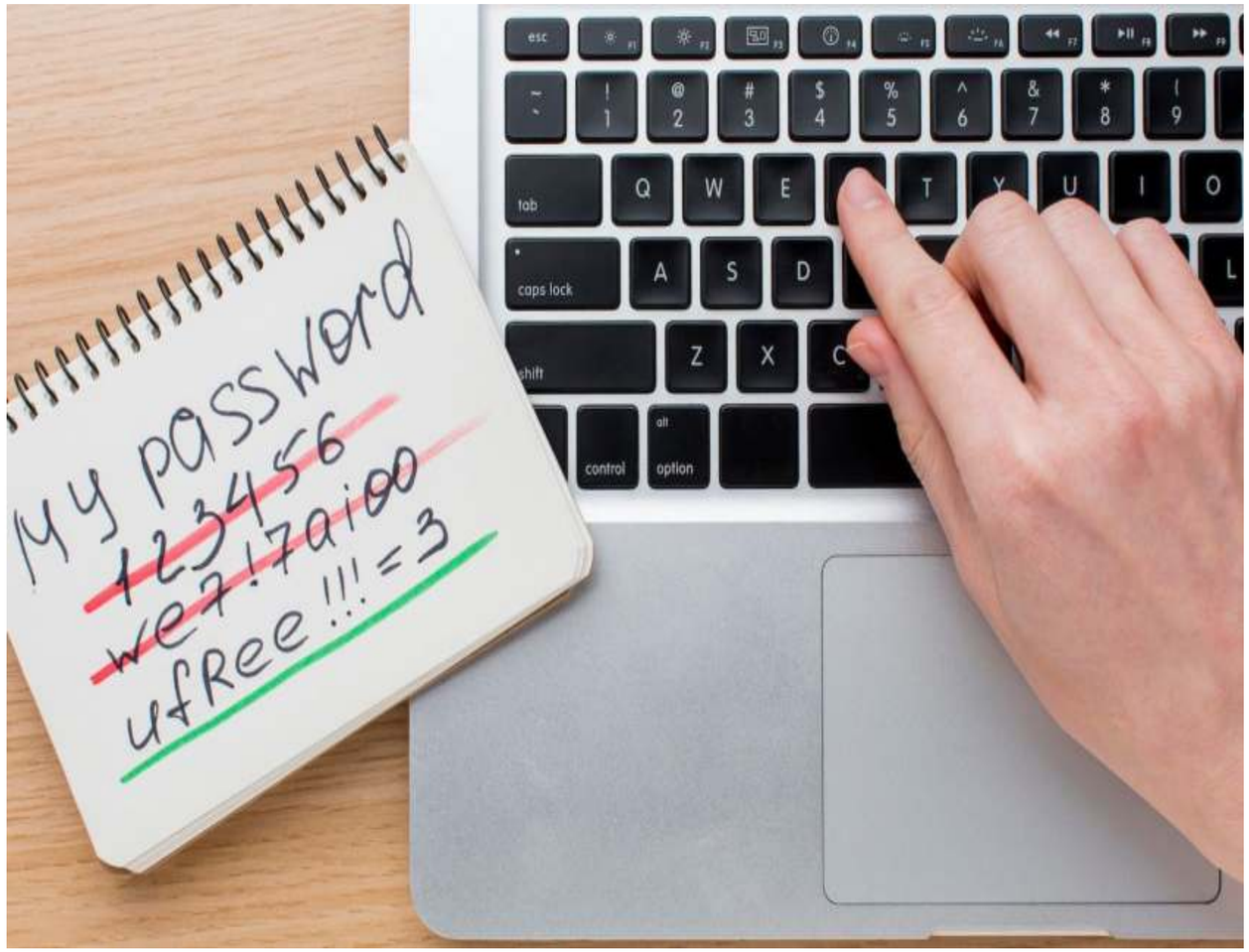
Как и большинство других мошеннических приемов, претекстинг нацелен не на взлом компьютера, а на использование уязвимостей нашей психики — чтобы сработал человеческий фактор. Ключевой момент — предварительная переписка с мошенником. Это и отличает претекстинг от обычного фишинга

7.Уэйлинг

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



ПРИЗНАКИ ФИШИНГА



Важно знать, как распознать фишинг. Признаки включают **неправильные адреса** отправителей, **грамматические ошибки** и **срочные запросы** на информацию. **Будьте внимательны к любым подозрительным сообщениям.**

РИСКИ ФИШИНГА

Фишинг может привести к серьезным финансовым потерям и утечке конфиденциальной и личной информации. Злоумышленники могут использовать ваши данные для кражи идентичности или доступа к информации и вашим счетам. Защита от фишинга — это необходимость.

Примеры фишинговых писем

1. **Тема, контент письма, названия файлов побуждают получателя к спешке, к немедленному действию** (к переходу по ссылке, к нажатию на кнопку, к открытию файла, к немедленному ответу на письмо).

   Здесь в полную меру используются эмоции, чувства, страхи, рефлексы.

   Например,

   - «У Вас не погашен кредит», «Ваше сообщение не доставлено», «Ваша почта будет заблокирована» - используется страх,
   - «Получи бесплатный лотерейный билет» - используется любопытство.

2. **В подписи к письму обычно нет обратного телефона отправителя**, либо вообще не указан отправитель.
3. **Обращение к получателю обычно обезличенное** (если это не целевой фишинг)

   Например, «Dear Ladies an Gentlemen», «Good afternoon», «Здравствуйте», «Уважаемый клиент»

Примеры фишинговых писем

4. **В письме используется автоподстановка для обращения к получателю**
   Например, «Dear <имя почтового ящика (до символа @)>»
5. **Часто письма отправляются от имени известных компаний** (логистических компаний, банков, платежных систем, органов судебной или исполнительной власти, олимпийских комитетов), **известных людей** (указание таких отправителей тоже воздействует на психологию получателей, так как вызывает рефлекторное доверие).
6. **Отправители**, выдают себя за официальных представителей известных компаний (в том числе, выдают себя за Ваших коллег), **но пишут с общих почтовых доменов gmail.com, mail.ru** и т.п., а не с корпоративных адресов
7. **Письмо требует ввести конфиденциальные данные**
8. **Письмо содержит какие-то документы, которые надо открыть** (например, либо какие-то «счета» - «invoice.doc», «Penalty Receipt.docm», либо просто какие-то документы «New doc 115.docm», «unnamed document.docm», якобы сканкопии. Вложения могут быть в виде doc, docm, pdf-файлов, архивов arj, zip, rar, исполняемых exe-файлов и в других форматах)

Примеры фишинговых писем

9. **Письмо содержит ссылки**, в том числе, замаскированные под изображения, документы, QR-коды, **и другие активные объекты** (кнопки и т.п.), переводящие на другие сайты или загружающие файлы.

10. **Текст ссылок в письме не совпадает с реальными ссылками**

11. **Строка адреса сайта в ссылке содержит спецсимвол «@» или другие странные символы**

Например, такой адрес http://google.com@fishing.com/anything означает, что ссылка Вас направит на сайт fishing.com, а не на google.com

МЕТОДЫ ЗАЩИТЫ

Для защиты от фишинга используйте двухфакторную аутентификацию и всегда проверяйте адреса сайтов. Не переходите по ссылкам из неизвестных источников и будьте осторожны с личной информацией

(Двухфакторная аутентификация с помощью приложения Яндекс-ключ, также двухфакторка будет организована в корпоративном портале Самарской области)

ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Установите антивирусное программное обеспечение и фильтры для электронной почты, чтобы защитить себя от фишинга. Эти инструменты могут помочь обнаружить и блокировать подозрительные сообщения до их открытия.

ЧТО ДЕЛАТЬ ПРИ АТАКЕ?

Если вы стали жертвой фишинга, немедленно измените пароли на всех учетных записях и сообщите об инциденте в службу поддержки. Также рекомендуется мониторить свои ресурсы на предмет подозрительной активности.

БУДУЩЕЕ ФИШИНГА

Фишинг продолжает эволюционировать с появлением новых технологий. Злоумышленники становятся все более изобретательными, и важно оставаться в курсе последних тенденций для эффективной защиты.

ЗАКЛЮЧЕНИЕ

Защита от фишинга требует внимания и осведомленности. Следуйте рекомендациям и оставайтесь бдительными, чтобы предотвратить мошенничество и защитить свою личную информацию. Будьте осторожны в цифровом мире.