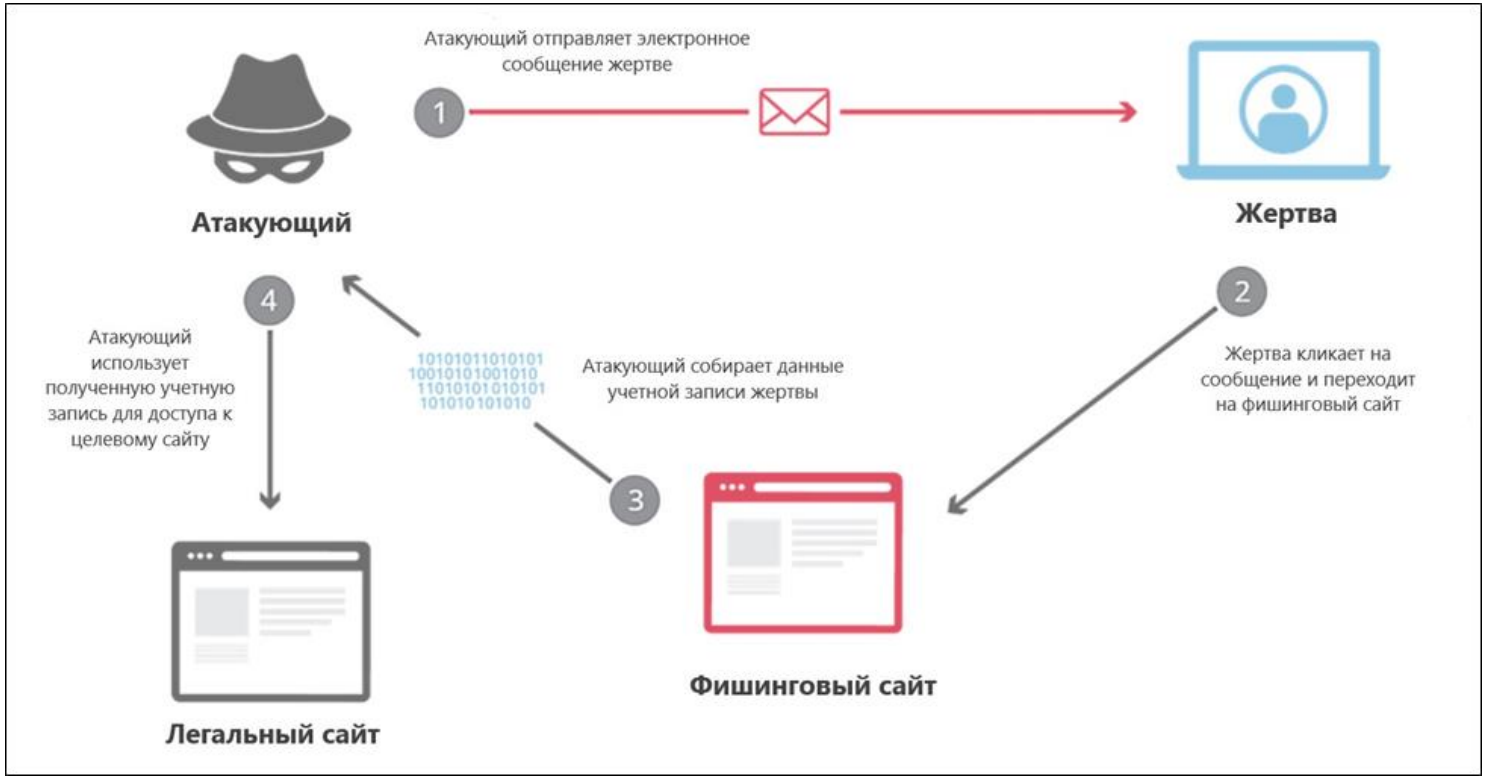
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Киберквест на Ampire: Управление рисками и фишинг. Как минимизировать угрозы в современном цифровом мире.

Яна Баринова
АО «Перспективный мониторинг»

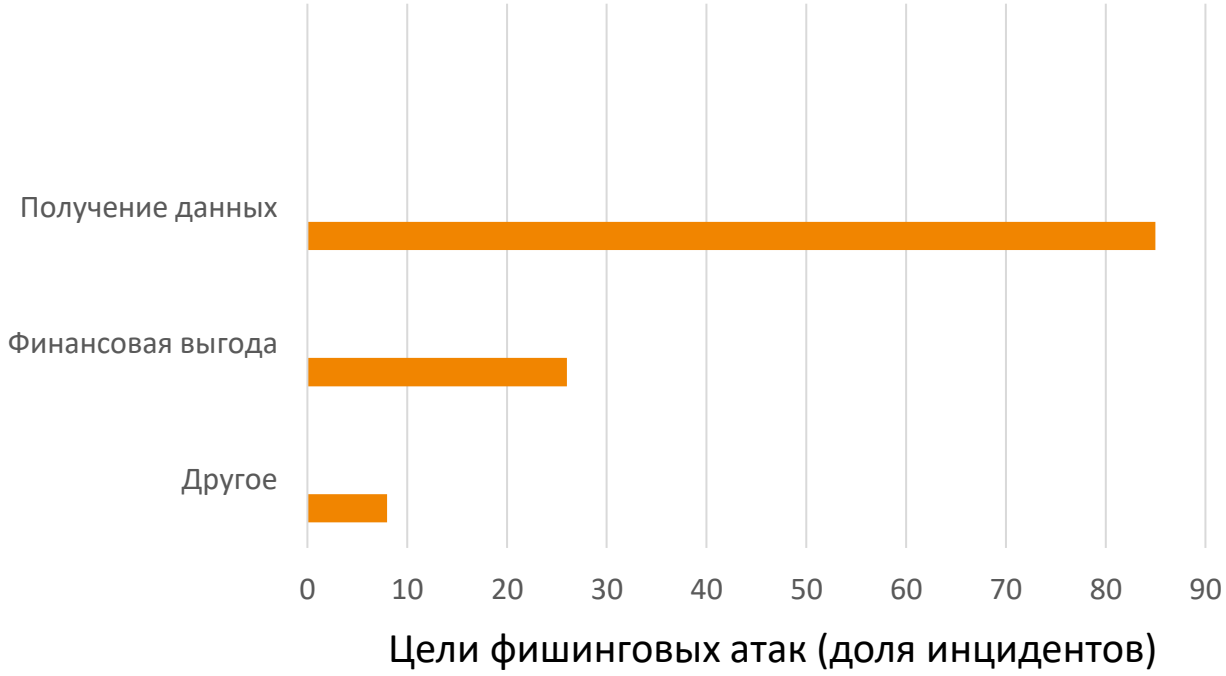
Модель атаки

Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности.



Тренды фишинговых атак

- Основной целью фишинговых атак является кража данных.
- В топ 3 вошли государственные учреждения, оборонно-промышленные предприятия и организации в сфере науки и образования.
- Самым распространенным способом доставки вредоносных сообщений по-прежнему является электронная почта.
- Фишинговые ссылки зачастую ведут на поддельную страницу для ввода данных.



Source: PT. Тренды фишинговых атак на организации в 2022–2023 годах

Виды фишинга

Почтовый фишинг

Голосовой фишинг

Подделка доменного имени

Клон-фишинг

SMS-фишинг

Фишинг в соцсетях и мессенджерах

Как противостоять фишингу?

Как распознать фишинговое письмо?

1. **Вы не ждали это письмо**

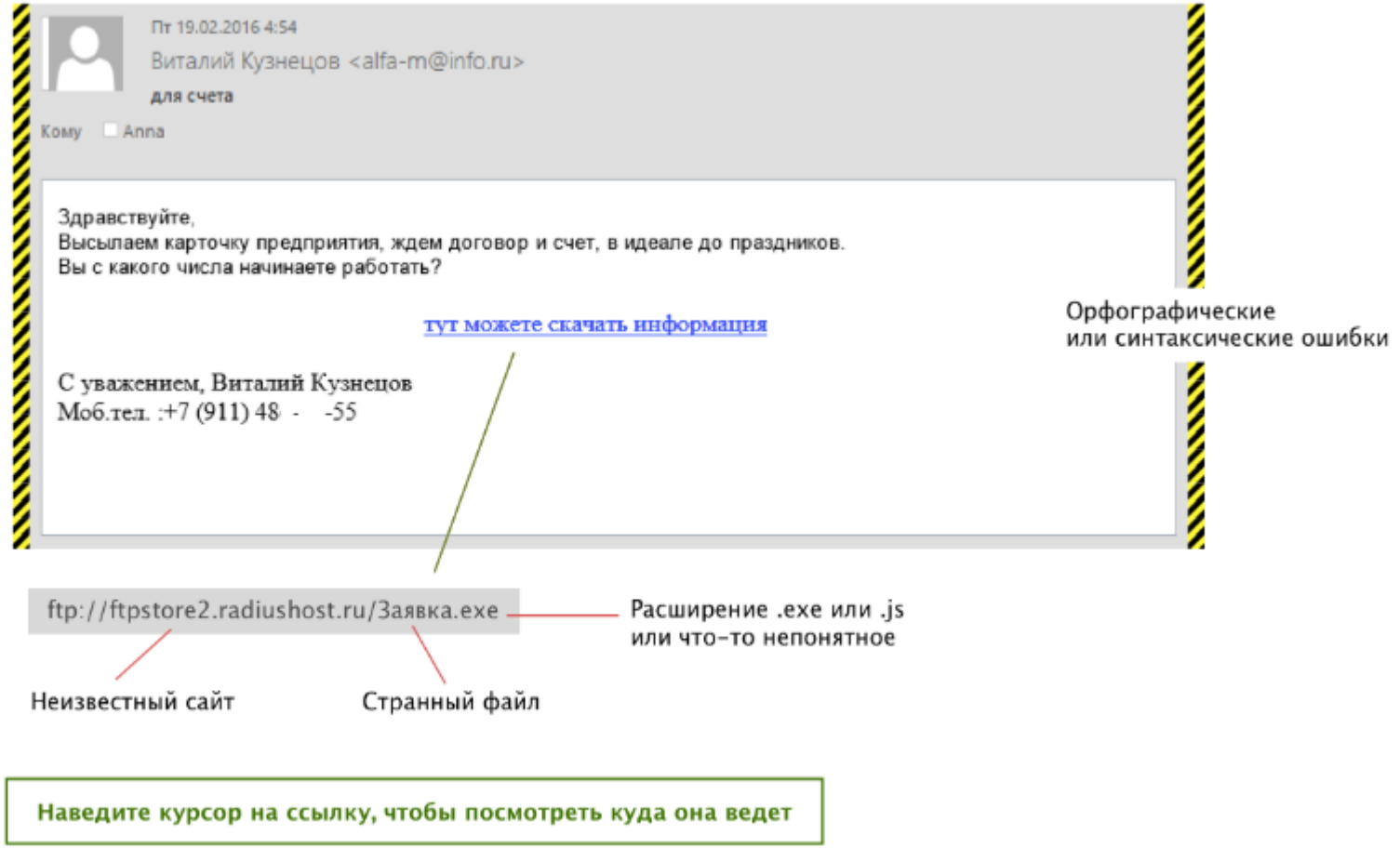
   Вы не знаете
   отправителя лично

2. **В письме — проблема или срочный вопрос**

   Вы узнали о проблеме
   из этого письма

   От вас требуется
   срочное действие

3. **Вас просят перейти по ссылке**



Наведите курсор на ссылку, чтобы посмотреть куда она ведет

Как можно избежать?

Остановитесь и подумайте

Социальные инженеры часто используют иллюзию срочности в расчете на то, что жертва не будет особо задумываться о происходящем. Всего минута размышлений может помочь вам выявить и предотвратить атаку.

Проверяйте источник

Например, посмотреть на заголовок электронного письма и сравнить его с другими письмами того же отправителя. Проверьте, куда ведут ссылки, – поддельные гиперссылки легко выявить, просто наведя на них курсор

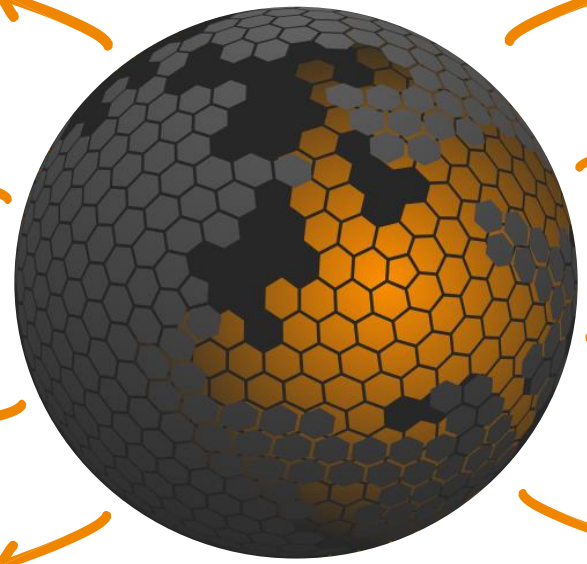
Насколько это правдоподобно?

Некоторые социальные инженеры рассчитывают на то, что вы не станете вдумываться. Попробуйте оценить, насколько реалистична ситуация, – так вы можете избежать атаки.

Защитите свои устройства

Регулярно обновляйте ПО, прошивки и защиту от вирусов. Для самых важных учетных записей используйте двухфакторную аутентификацию.

Экосистема Ampire



Исследование защищенности

Red Team

Специалисты проактивной защиты

Средства защиты

Разработчики СЗИ

Цифровая грамотность

Ampire Junior

OSINT
Непрофильные пользователи

Реагирование на инциденты

CSIRT

Специалисты SOC

Киберучения

ИТ/ИБ специалисты

Blue Team

Киберквесты

Начинающие специалисты

Конфигуратор и УУ

Разработчики
DevOps инженеры

Отраслевые шаблоны

Отраслевые ИТ/ИБ специалисты

- Офис промышленного предприятия
- АСУ ТП ВАПС (Электроэнергетика)
  Телеком (ОКС-7)
  Телеком (SIP-телефония)
- АСУ ТП (Топливно-промышленный комплекс)
- Импортозамещение

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Сообщество Ampire

Спасибо
за внимание!

t.me/pm_public @AMonitoring ampire.team

Баринова Яна
Специалист по информационной безопасности

+7 (495) 737-61-97
info@amonitoring.ru