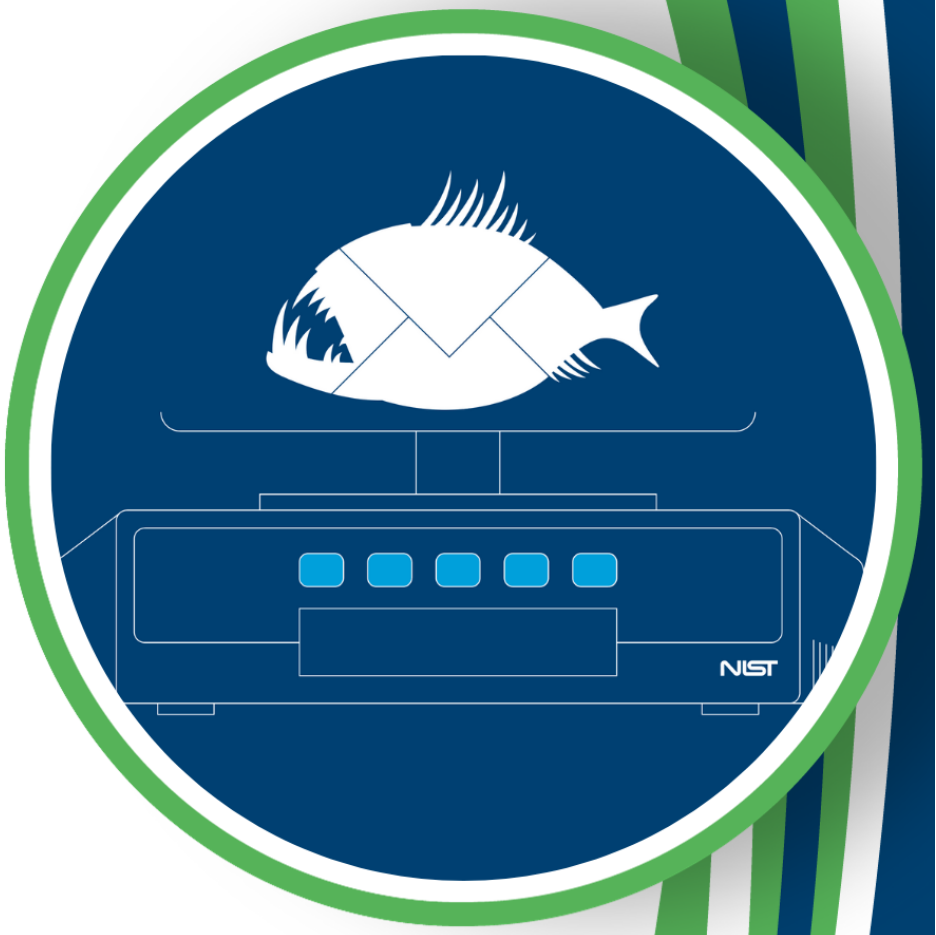
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST PHISH SCALE
USER GUIDE

Prepared By:
Shanée Dawkins
Jody Jacobs



DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

Техническое примечание НИСТ

НИСТ ТН 2276

Руководство пользователя шкалы Фиша NIST

Шэни Докинз

Группа визуализации и удобства использования, Отдел доступа к информации

Лаборатория информационных технологий

Джоди Джейкобс

Группа визуализации и удобства использования, Отдел доступа к информации

Лаборатория информационных технологий

Данная публикация доступна бесплатно по адресу:
https://doi.org/10.6028/NIST.TN.2276

ноябрь 2023 г.

Министерство торговли США

Джина М. Раймондо, секретарь

Национальный институт стандартов и технологий

Лори Э. Локасио, директор NIST и заместитель министра торговли по стандартам и технологиям

НИСТ ТН 2276

ноябрь 2023 г.

Определенное коммерческое оборудование, инструменты, программное обеспечение или материалы, коммерческие или некоммерческие, идентифицируются в этой статье для адекватного описания экспериментальной процедуры. Такая идентификация не подразумевает рекомендации или одобрения какого-либо продукта или услуги со стороны NIST, а также не означает, что материалы или идентифицированное оборудование обязательно является лучшим из имеющихся для этой цели..

Правила технической серии NIST

Положения об авторских правах, использовании и лицензировании
Синтаксис идентификатора публикации технической серии NIST

История публикаций

Утверждено редакционным советом NIST 8 ноября 2023 г.

Как цитировать эту публикацию технической серии NIST

Докинз С., Джейкобс Дж. (2023) Руководство пользователя шкалы Фиша NIST. (Национальный институт стандартов и технологий, Гейтерсбург, Мэриленд), NIST Series TN 2276.https://doi.org/10.6028/NIST.TN.2276

Идентификаторы ORCID автора NIST

Шэни Докинз: 0000-0002-8114-0608
Джоди Джейкобс: 0000-0002-6433-884X

Контактная информация

human-cybersec@nist.gov

НИСТ ТН 2276

ноябрь 2023 г.

Абстрактный

Фишинговые киберугрозы затрагивают частный и государственный секторы как в США, так и за рубежом. Встроенные программы обучения осведомленности о фишинге, в которых сотрудникам рассылаются симулированные фишинговые электронные письма, предназначены для подготовки сотрудников этих организаций к борьбе с реальными сценариями фишинга. Специалисты и специалисты по обучению кибербезопасности и фишингу частично используют результаты этих программ для оценки риска безопасности своей организации. Шкала фишинга NIST — это метод, созданный для этих разработчиков для оценки сложности обнаружения фишинга в электронных письмах в рамках своих программ обучения кибербезопасности и фишингу. В этом руководстве пользователя полностью описана шкала фишинга, а также приведены инструкции по ее применению к фишинговым электронным письмам. Кроме того, приложения включают 1) рабочие листы, которые помогут специалистам по обучению применению шкалы Фиша, и 2) подробную информацию о свойствах электронной почты и соответствующие исследования в литературе.

Ключевые слова

Компрометация деловой электронной почты (BEC); Информационная безопасность; Кибербезопасность, ориентированная на человека; шкала Фиша; Фишинг; Социальная инженерия; Полезная безопасность, Полезная кибербезопасность.

Оглавление

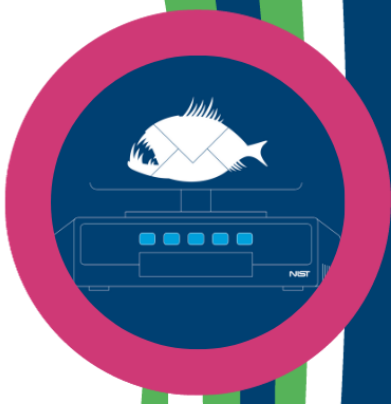
Список таблиц

список рисунков

Благодарности

NIST хотел бы выразить признательность Мишель Стивс, Кристен Грин, Мэри Теофанос и Дженнифер Костик за их усилия по разработке шкалы Фиша NIST. Авторы также хотели бы поблагодарить Ферн Барриентос, Сюзанну Фурман и Кевина Мэнголда за их вклад в разработку данного руководства пользователя. Особая благодарность руководителям программ обучения по борьбе с фишингом, которые предоставили отзывы об использовании этого документа в своих организациях.

1. Introduction



Фишинг — это угроза кибербезопасности, основанная на электронной почте, при которой киберпреступники пытаются получить конфиденциальную информацию от получателей электронной почты. Это метод социальной инженерии, который заставляет получателя электронной почты выполнить действие, выгодное злоумышленнику (например, щелкнуть ссылку на мошеннический веб-сайт или загрузить вредоносное вложение) [17]. Фишинговые киберугрозы затрагивают частный и государственный сектора как в Соединенных Штатах (США), так и за рубежом. Это остается одной из главных угроз безопасности для этих организаций, обходясь компаниям в миллиарды [11]. Поскольку технологические средства защиты и фильтры электронной почты не гарантированно блокируют все входящие вредоносные электронные письма, люди часто являются последней линией защиты организации от фишинговых атак. Поэтому крайне важно, чтобы сотрудники этих организаций были готовы к реальным сценариям фишинга.

Встроенные программы обучения по вопросам фишинга предназначены для борьбы с угрозами фишинга. В этих программах сотрудникам рассылаются симулированные фишинговые электронные письма, чтобы научить их распознавать настоящие фишинговые электронные письма, которые они могут получить. Персонал, выполняющий такие программы, именуемый в настоящем Руководстве пользователя «специалистами по обучению», частично использует результаты этих программ для оценки риска безопасности своей организации. Эти результаты обычно измеряются с помощью *рейтинг кликов*–количество людей, которые нажали на потенциально вредоносную ссылку или вложение, из общего числа людей, отправивших симулированное фишинговое письмо, и *ставки отчетности*–количество людей, сообщивших о подозрительном электронном письме в свою организацию, из общего числа людей, отправивших симулированное фишинговое письмо. Однако количество кликов и количество отчетов не дают полной картины риска фишинга в организации; они дают единую информацию — какой процент людей «попался» на фишинг. Тот факт, что некоторые фишинговые электронные письма людям труднее обнаружить, чем другие, можно учитывать при оценке имитационных учебных упражнений по фишингу, предоставляя дополнительный показатель при оценке общего риска кибербезопасности. Метод, описанный в данном руководстве пользователя, решает эту проблему.

Шкала фишинга NIST — это метод обучения разработчиков оценивать сложность обнаружения фишинга в электронных письмах, оценивая как свойства самого фишингового письма, так и характеристики получателей электронного письма.

Шкала Фиша NIST, именуемая в дальнейшем Шкала Фиша, была первоначально опубликована в исследовательской статье в 2019 году.[1][22], расширен в исследовательском журнале в 2020 году [23] и дополнительно изучен в последующие годы [3] [4]. В этих публикациях подробно рассказывается о том, как шкала фишинга была создана с использованием эмпирических данных моделирования фишинга, а также об исследованиях, лежащих в основе ее оценки с помощью обучения специалистов по внедрению. Данное руководство пользователя служит первым шагом на пути перехода от исследований к практике, полностью описывая шкалу фишинга и предоставляя инструкции по ее применению к фишинговым электронным письмам. Рабочий лист для помощи специалистам по обучению применению Phish

[1] Предыдущее исследование NIST показало, что пользовательский контекст играет ключевую роль в интерпретации частоты кликов [9].

Масштаб представлен в Приложении А. Подробная информация о свойствах электронной почты и соответствующих исследованиях в литературе представлена в Приложении Б.

1.1. Использование данного руководства пользователя

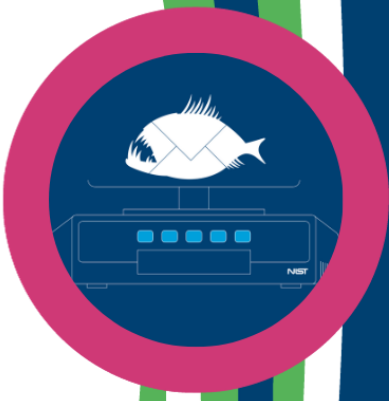
Настоящее Руководство пользователя предназначено для использования специалистами-практиками – специалистами по обучению по вопросам фишинга, специалистами по обучению по вопросам кибербезопасности и другими специалистами по компьютерной безопасности, ответственными за проведение учебных занятий по фишингу (например, проектирование, выполнение и/или анализ данных). Рейтинг сложности обнаружения фишинга человеком, полученный в результате применения шкалы фишинга, помогает специалистам по обучению осведомленности о фишинге двумя основными способами:

1. Предоставляя контекст относительно показателей кликов обучающих сообщений и показателей отчетов для целевой аудитории, и
2. Предоставляя способ охарактеризовать реальные фишинговые угрозы, чтобы организатор обучения мог снизить риск безопасности организации, адаптируя обучение к типам угроз, с которыми сталкивается его организация [22].

Хотя это руководство было разработано с использованием эмпирических данных [22], при рассмотрении вопроса об использовании шкалы Фиша организаторы обучения должны адаптировать метод к текущей среде своей организации и численности сотрудников. Кроме того, при применении шкалы фишинга к электронной почте важно, чтобы организатор обучения был последовательным в своих оценках, чтобы обеспечить эффективность сравнения сложности обнаружения фишинга людьми в разных электронных письмах.

Фишинг — это лишь один из аспектов общей программы кибербезопасности, проводимой организатором обучения. Принимая во внимание программу обучения и осведомленности о кибербезопасности организации в целом, шкала фишинга является дополнительным показателем, который специалисты по обучению могут использовать для снижения риска безопасности своей организации, сохраняя при этом миссию своей организации и толерантность к риску.

2. The NIST Phish Scale



Шкала фишинга состоит из двух основных компонентов, используемых вместе для определения сложности обнаружения фишинга со стороны человека [22]:

1. Система оценки наблюдаемых характеристик самого фишингового письма.
2. Система оценки соответствия посыла фишингового письма целевой аудитории.

Первый компонент измеряется путем оценки визуальных индикаторов (подсказок), присутствующих в электронном письме, которые могут предупредить получателей электронной почты при обнаружении фишинга, таких как количество подсказок, характер подсказок и повторение подсказок. Второй компонент – согласование предпосылок – основан на текущих событиях, среде организации, а также ролях и обязанностях получателя. Оба компонента сначала измеряются, а затем интерпретируются вместе, что приводит к общему рейтингу сложности обнаружения человеком фишингового электронного письма. В разделах 2.1–2.3 подробно описаны эти компоненты с инструкциями о том, как определить общую сложность обнаружения фишинга человеком для фишингового электронного письма.

2.1. Электронная почта

Первый компонент шкалы фишинга — это система оценки наблюдаемых характеристик самого фишингового электронного письма, называемого электронной почтой.*подсказки*[22].

Сигналы — это свойства электронного письма, которые либо заставляют пользователя щелкнуть мошенническую ссылку или вложение, либо предупреждают пользователя о том, что электронное письмо может быть фишинговым. Меньшее количество признаков в фишинговом электронном письме указывает на то, что кому-то труднее обнаружить фишинговое письмо; большее количество сигналов указывает на более легкое обнаружение.

Подсказки в электронном письме обеспечивают объективную оценку самого электронного письма; количество сигналов, присутствующих в электронном письме, классифицируется по этому компоненту шкалы Фиша. Эта категория сигналов вместе с категорией соответствия помещения электронного письма используется для определения сложности обнаружения. При классификации количества сигналов в фишинговом электронном письме важно сначала понять, какие типы сигналов могут присутствовать в фишинговом электронном письме и где они встречаются.

2.1.1. Список сигналов

Фишинговые сигналы электронной почты делятся на пять типов [22]:

1. Ошибки – связанные с орфографическими и грамматическими ошибками и несоответствиями, содержащимися в сообщении;

2. Технические индикаторы – относящиеся к адресам электронной почты, гиперссылкам и вложениям;

3. Индикаторы визуальной презентации – относящиеся к брендингу, логотипам, дизайну и форматированию;

4. Язык и содержание – например, общее приветствие и отсутствие данных о подписывающем лице, использование нехватки времени и угрожающие выражения; и

5. Распространенная тактика – использование гуманитарных призывов, предложений «слишком хорошо, чтобы быть правдой», ограниченных по времени предложений, выдачи себя в роли друга, коллеги или авторитетного деятеля и т.п.

Каждый тип сигнала имеет связанные сигналы, всего 23, перечисленные в Таблице 1. Более подробную информацию о сигналах и о том, что искать в электронном письме, можно найти в Приложении B.

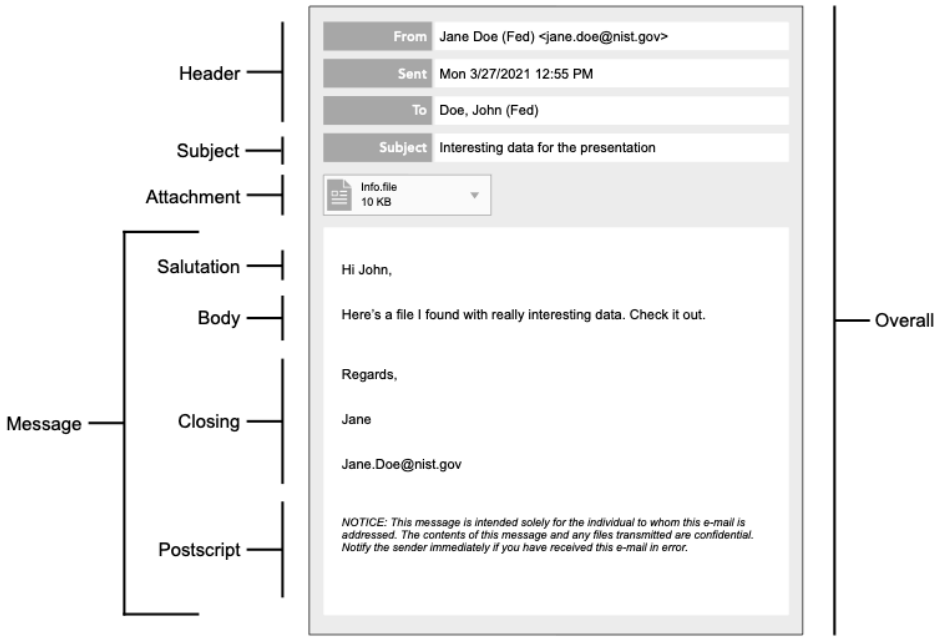
Таблица 1. Список сигналов по типам

Тип сигнала	Имя сигнала
Ошибка	Орфографические и грамматические нарушения
	непоследовательность
Технический индикатор	Тип прикрепления
	Отображаемое имя и адрес электронной почты отправителя
	URL-гиперссылка
	Подмена домена
Индикатор визуального представления	Брендинг и логотипы отсутствуют/минимальны
	Имитация логотипа или устаревший брендинг/логотипы
	Непрофессиональный дизайн или форматирование
	Индикаторы и значки безопасности
Язык и содержание	Юридический язык/информация об авторских правах/отказ от ответственности
	Отвлекающие детали
	Запросы конфиденциальной информации
	В срочном порядке
	Угрожающий язык
	Общее приветствие
	Отсутствие данных о подписанте
Общая тактика	Гуманитарные обращения
	Слишком хорошие, чтобы быть правдой предложения
	Ты особенный
	Ограниченное по времени предложение
	Имитирует рабочий или бизнес-процесс
	Выдает себя за друга, коллегу, начальника, авторитетную фигуру

2.1.2. Определение сигналов

При анализе электронного письма важно понимать, как правильно идентифицировать его сигналы. В то время как гл. 2.1.1 указаны характеристики каждого сигнала. В этом разделе рассматривается анатомия электронной почты и подчеркивается, где обычно встречаются различные типы сигналов. На рисунке 1 показан пример фишингового письма. В целом электронное письмо состоит из четырех основных компонентов:

- Заголовок – включает в себя *От*, *Отправил*, и *К* информация
- Предмет
- Вложение – если присутствует, один или несколько загружаемых файлов.
- Сообщение – включая приветствие (приветствие), тело (основное содержание), закрытие (подпись).



Типы сигналов «Ошибка» и «Технический индикатор» можно найти в любом месте электронного письма, в зависимости от сигнала. Типы сигналов «Индикатор визуального представления» связаны с тем, как отображается электронное письмо, и поэтому обычно встречаются в сообщении электронной почты. Типы подсказок «Язык и содержание» и «Общая тактика» больше связаны с предпосылкой электронного письма и расположены в теме или сообщении электронного письма. См. Приложение B, где указано типичное расположение отдельных сигналов.[2].

2.1.3. Классификация количества сигналов

Категоризация сигналов зависит от количества наблюдаемых сигналов в фишинговом электронном письме. Фишинговое электронное письмо следует тщательно изучить, чтобы обнаружить и идентифицировать присутствующие признаки. Для этого используйте критерии, приведенные в Таблице 2, подсчитывая каждый экземпляр сигналов, присутствующих в фишинговом электронном письме. Например, если

[2] Из-за различных почтовых клиентов, настройки электронной почты пользователя и устройства, на котором пользователи будут просматривать свою электронную почту, расположение подсказок может различаться.

в фишинговом письме есть три орфографические и две грамматические ошибки, в общее количество реплик засчитываются пять «орфографических и грамматических нарушений». Обратите внимание, что некоторые характеристики электронной почты можно идентифицировать и учитывать как несколько сигналов. Например, электронное письмо с гиперссылкой, отображаемой как «www.niist.gov» (в отличие от реального домена www.nist.gov), имеющее базовый унифицированный указатель ресурса (URL) на «commerce.gov», будет считаться как как подсказки «Орфографические и грамматические нарушения», так и «Гиперссылки URL». Оцените фишинговое письмо, подсчитав количество сигналов, присутствующих в письме, и суммируя общее количество сигналов. Форму, включенную в Приложение А, можно использовать в качестве рабочего листа, который поможет вам подсчитывать сигналы.

Таблица 2. Критерии подсчета сигналов

Тип сигнала	Имя сигнала	Критерии подсчета
Ошибка	Орфография и грамматика нарушения	Содержит ли сообщение орфографические или грамматические ошибки, включая несовпадающее множество слов?
	непоследовательность	Есть ли в сообщении электронной почты несоответствия?
Технический индикатор	Тип прикрепления	Есть ли потенциально опасное вложение?
	Отображаемое имя и адрес электронной почты отправителя	Скрывает ли отображаемое имя реальный адрес отправителя или адрес электронной почты для ответа?
	URL-гиперссылка	Есть ли текст, который скрывает за текстом истинный URL-адрес?
	Подмена домена	Является ли доменное имя, используемое в адресах или ссылках, похожим на домен законного лица?
Визуальный презентация индикатор	Брендинг и логотипы отсутствуют/ минимальны	Отсутствуют ли соответствующие фирменные маркировки, символы или знаки отличия?
	Имитация логотипа или устаревший брендинг/логотипы	Не кажутся ли какие-либо элементы брендинга имитацией или устаревшими?
	Непрофессиональный вид дизайн или форматирование	Нарушает ли дизайн и форматирование какие-либо общепринятые профессиональные практики? Кажется, что элементы дизайна созданы непрофессионально?
	Индикаторы и значки безопасности	Имеются ли какие-либо маркеры, изображения или логотипы, предполагающие безопасность электронной почты?
Язык и контент	Юридический язык/информация об авторских правах/отказ от ответственности	Содержит ли сообщение какие-либо юридические формулировки, такие как информация об авторских правах, отказ от ответственности или налоговая информация?
	Отвлекающие детали	Содержит ли электронное письмо лишние или не связанные с основной посылом детали?
	Запросы на конфиденциальную информацию информация	Содержит ли сообщение запрос какой-либо конфиденциальной информации, включая личную информацию или учетные данные?
	В срочном порядке	Содержит ли сообщение нехватку времени, чтобы заставить пользователей быстро выполнить запрос, включая подразумеваемое давление?
	Угрожающий язык	Содержит ли сообщение угрозу, в том числе подразумеваемую, например, юридические последствия бездействия?
	Общее приветствие	В сообщении отсутствует приветствие или персонализация сообщения?
	Отсутствие данных о подписанте	В сообщении отсутствуют сведения об отправителе, например контактная информация?
Общий тактика	Гуманитарные обращения	Содержит ли сообщение призыв помочь нуждающимся?
	Слишком хорошие, чтобы быть правдой предложения	Предлагает ли сообщение что-то слишком хорошее, чтобы быть правдой, например, выигрыш в конкурсе, лотерее, бесплатный отпуск и так далее?
	Ты особенный	Предлагает ли вам электронное письмо что-нибудь специально для вас, например валентинку от тайного поклонника?
	Ограниченное по времени предложение	Предлагает ли электронное письмо что-то, что не продлится долго или ограниченный период времени?
	Имитирует рабочий или бизнес-процесс	Похоже ли сообщение на рабочий или деловой процесс, например новое голосовое сообщение, доставка посылки, подтверждение заказа, уведомление о счете?
	Выдает себя за друга, коллегу, начальника, авторитетную фигуру	Похоже, что сообщение пришло от друга, коллеги, начальника или другого авторитетного лица?

Шкала Фиша имеет три категории, которые соответствуют общему количеству сигналов:

- Мало – фишинговое электронное письмо содержит меньше признаков и меньше возможностей идентифицировать электронное письмо как фишинговое.
- Некоторые – фишинговое письмо содержит умеренное количество намеков.
- Много – фишинговое письмо имеет большее количество признаков и больше возможностей идентифицировать письмо как фишинговое.

Используйте сопоставление, приведенное в таблице 3, чтобы определить категорию сигнала фишингового письма на основе общего количества сигналов для этого письма.

Таблица 3. Сопоставление категорий сигналов фишинговой электронной почты

Общее количество сигналов	Категория сигнала
1–8 сигналов	Мало (сложнее)
9–14 реплик	Некоторый
15 и более реплик	Многие (менее сложные)

Категория сигналов «несколько», «несколько» или «много» переносится в разд. 2.3, Определение сложности обнаружения, а также согласование предпосылок, которое подробно рассматривается далее в разд. 2.2.

2.2. Выравнивание помещения

Второй компонент шкалы фишинга фокусируется на взаимосвязи между пользовательским контекстом и фишинговым сообщением электронной почты.*выравнивание помещения*[22]. Когда связь сильна, это близко к тому, что часто называют целевым фишингом.

Согласованность помещения — это мера того, насколько близко электронное письмо соответствует рабочим ролям или обязанностям получателя или организации электронного письма. Чем сильнее соответствует посылу электронное письмо, тем труднее его обнаружить как фишинг. И наоборот, чем слабее содержание электронного письма, тем легче его обнаружить как фишинг.

Оценка соответствия предпосылки фишингового электронного письма — это процесс определения релевантности предпосылки сообщения электронной почты для*целевая аудитория*. Этот*целевая аудитория*может быть сосредоточен на одном из

различные уровни внутри вашей организации (например, подразделения, отделы, группы, команды) для контекстуализации показателей кликов и их прямой связи с конкретными отделами или сотрудниками. Расположение помещения невозможно оценить без знания*целевая аудитория*контекст работы относительно сути фишингового сообщения электронной почты. Таким образом, измерение целостности фишингового электронного письма должно выполняться человеком, обладающим знаниями в области*целевая аудитория* культура труда и ответственность.

Измерение соответствия предпосылки фишингового электронного письма начинается с присвоения числового значения (оценки применимости) пяти отдельным элементам соответствия предпосылке. Затем с использованием этих оценок применимости рассчитывается рейтинг соответствия помещения. Этот окончательный рейтинг соответствия предпосылок затем сопоставляется с категорией сильного, среднего или слабого соответствия предпосылок, которая, рассматриваемая с категорией сигналов, используется для определения сложности обнаружения электронного письма. Прежде чем оценивать фишинговое электронное письмо, необходимо понять пять элементов, лежащих в основе этого процесса. Описание этих элементов и способы их использования для расчета рейтинга выравнивания помещения приведены в разделах ниже. Форма рабочего листа, включенная в Приложение А, может быть использована для помощи специалистам по обучению измерению соответствия электронной почты предпосылкам.

2.2.1. Элементы выравнивания помещения

Каждый из пяти элементов выравнивания помещений подробно описан ниже.

Элемент 1 – Имитирует процесс или практику на рабочем месте

Этот элемент отражает актуальность темы электронного письма для процесса или практики целевой аудитории. Для этого элемента следует учитывать любые процессы или функции, которые обычно происходят в вашей организации.

Например, если целевая аудитория обычно получает официальные уведомления чата организации через приложение, электронное письмо, уведомляющее получателя о пропущенном сообщении чата, будет иметь более низкий балл применимости для этого элемента. Однако если электронная почта является типичным механизмом уведомлений чата, эта электронная почта будет иметь более высокий балл применимости для этого элемента.

Элемент 2 – Имеет актуальность на рабочем месте

Этот элемент отражает актуальность помещения для работы целевой аудитории, включая их роли и обязанности. Крайне важно знать должностные обязанности и должностные функции вашей целевой аудитории, чтобы правильно оценить этот элемент.

Например, если целевой аудиторией является финансовый отдел, а в электронном письме содержится предпосылка о просроченном или пропущенном платеже, это электронное письмо будет иметь более высокий балл применимости для этого элемента. Еще одним фактором, учитывающим этот элемент, является домен отправителя. Если доменное имя отправителя электронной почты совпадает или похоже на домен вашей организации (например, john.doe@nist.gov получает электронное письмо от jane.doe@nist.gov), электронное письмо будет иметь более высокий балл применимости. для этого элемента. Хотя политики безопасности многих организаций запрещают или не одобряют использование личной электронной почты в деловых целях, по-прежнему достаточно распространена практика, согласно которой для этого элемента следует рассматривать отправителей со знакомыми именами и общедоступными доменами. Если целевая аудитория знакома с сотрудником вашей организации, например, с руководителем по имени Джон Доу, то электронное письмо с адреса « john.doe@gmail.com » будет иметь более высокий балл применимости.

Также подумайте, имеет ли электронное письмо отношение к работе и обязанностям всей целевой аудитории или ее части. Например, если идея электронного письма имеет более высокую контекстуальную согласованность, но только для небольшой части целевой аудитории, то элементу релевантности на рабочем месте следует присвоить средний балл применимости.

Элемент 3 – Согласован с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту.

Этот элемент основан на времени получения фишингового письма целевой аудиторией. Он отражает соответствие предпосылки внутренним и внешним ситуациям или событиям, прямо или косвенно влияющим на вашу организацию. Примерами внешних событий, связанных с календарем, в США являются Рождество, Новый год и День памяти; примерами внутренних событий являются прием на работу нового директора/президента/руководителя организации, открытие нового филиала, а также начало или конец финансового года. Если событие актуально и актуально для целевой аудитории, то оценка применимости этого элемента должна быть выше (например, фишинговое письмо, отправленное примерно 14 февраля и связанное со Днем святого Валентина). И наоборот, если событие не является актуальным или неактуальным для целевой аудитории, то предпосылка должна иметь более низкий балл применимости (например, фишинговое электронное письмо о зимней праздничной вечеринке в офисе, отправленное в середине лета).

Элемент 4. Вызывает беспокойство по поводу последствий НЕ нажатия кнопки

Этот элемент отражает потенциально опасные последствия, если не будет предпринято никаких действий, что повышает вероятность того, что получатель фишингового письма нажмет на мошеннические ссылки или вложения. Определенные помещения электронной почты вызывают такую реакцию у получателей больше, чем другие. Например, фишинговое электронное письмо, вызванное страхом пользователя пропустить что-то (например, пропущенное сообщение, информационное уведомление), может не вызвать такого же ответа, как электронное письмо с более серьезным обвинением (например, о потенциальной утечке защищенной медицинской информации, раскрытии личной информации, программы-вымогатели). В первом случае оценка применимости этого элемента будет ниже, чем во втором.

Элемент 5. Был объектом целевого обучения, специальных предупреждений или иного воздействия.

Этот элемент отражает влияние обучения на целевую аудиторию, включая, например, организационное обучение, связанное с фишингом, по распознаванию и сообщению о фишинговых электронных письмах. В идеале сотрудники, прошедшие какое-либо обучение ИТ-безопасности, связанное с фишингом, будут более разумно идентифицировать электронное письмо как фишинговое (более высокий балл применимости для этого элемента), чем те, кто не прошел обучение (более низкий балл применимости для этого элемента). этот элемент). Обучение фишингу не ограничивается компонентами официальных учебных курсов по ИТ-безопасности; обучение относится к любым информационным материалам или руководствам, которым была подвергнута целевая аудитория. Обучение может относиться к:

- официальные программы повышения осведомленности и обучения в области ИТ-кибербезопасности [5][7][16][19][25];
- образовательные материалы или семинары о том, как распознать фишинговое письмо; или
- организационные электронные письма, предупреждающие сотрудников о необходимости быть в курсе попыток фишинга или предупреждающие об определенных типах фишинговых атак.

Если получатель фишингового письма прошел значительную подготовку по обнаружению фишинговых писем, этот элемент будет иметь более высокий балл применимости. Аналогично, оценка применимости будет высокой, если в организации существует надежная программа обучения по борьбе с фишингом в течение длительного периода времени.

2.2.2. Оценка элементов выравнивания помещения

Чтобы рассчитать рейтинг соответствия помещения, сначала присвойте каждому из пяти элементов соответствия помещения четное числовое значение от нуля до восьми – балл применимости (см. Таблицу 4). Элемент с нулевой оценкой применимости указывает на полное несоответствие релевантности элемента целевой аудитории. И наоборот, высокий балл применимости, равный восьми, указывает на то, что элемент очень применим к целевой аудитории.

Таблица 4. Шкала применимости планировки помещения

Шкала применимости[3]	Применимость Счет
Чрезвычайная применимость, согласованность или релевантность	8
Значительная применимость, согласованность или релевантность	6
Умеренная применимость, согласованность или релевантность	4
Низкая применимость, согласованность или релевантность	2
Не применимо, не согласовано или не релевантно	0

В Таблице 5 представлены критерии для пяти элементов выравнивания помещений. Используйте эти критерии вместе со шкалой применимости, чтобы определить оценку применимости для каждого элемента.

Таблица 5. Критерии оценки элементов планировки помещения

Элементы выравнивания помещения	Критерии оценки
1: Имитирует процесс или практику на рабочем месте.	Пытается ли этот элемент отразить соответствие помещения процессу или практике на рабочем месте для целевой аудитории?
2: Имеет отношение к рабочему месту	Пытается ли этот элемент отразить актуальность замысла для целевой аудитории?
3: Соответствует другим ситуациям или событиям, в том числе внешним по отношению к рабочему месту.	Соответствует ли этот элемент другим ситуациям или событиям, даже внешним по отношению к рабочему месту, придавая сообщению ощущение знакомости?
4. Вызывает беспокойство по поводу последствий НЕ нажатия	Отражает ли этот элемент потенциально вредные последствия отсутствия нажатия, повышающие вероятность нажатия?
5: Был объектом целевого обучения, специальных предупреждений или иного воздействия.	Отражает ли этот элемент целевые эффекты обучения, которые приведут к обнаружению помещений? Необходимо позаботиться о том, чтобы надлежащим образом учесть специфику обучения или предупреждения, поскольку передача знаний довольно сложна.

[3] Стивс и др. ал. использовал термин «якоря» в самой последней публикации о фишинговых масштабах [23]. В данном справочнике для ясности используется термин «шкала применимости».

Оценка применимости для каждого элемента выравнивания помещения используется для расчета окончательного рейтинга выравнивания помещения.

2.2.3. Категоризация выравнивания помещения

Оценки применимости из предыдущего раздела используются для расчета окончательного рейтинга соответствия предпосылок: суммируйте баллы применимости для элементов с первого по четвертый, затем вычитайте балл применимости для элемента 5 из общей суммы. Пятый элемент относится к обучению и помогает в обнаружении; поэтому числовое значение, присвоенное этому элементу, вычитается из общей суммы. Уравнение 1 ниже показывает расчет, необходимый для выравнивания помещения.

$$= (\quad 1 \ h \quad h \quad 4) - \quad 5 \qquad (1)$$

Наивысший возможный рейтинг соответствия помещения — 32, что указывает на то, что фишинговое сообщение электронной почты соответствует целевой аудитории, и целевая аудитория не прошла никакого соответствующего обучения и не получила никаких предварительных предупреждений или предупреждений о предстоящем фишинге. Наименьший возможный рейтинг соответствия предпосылок составляет -8, что указывает на то, что фишинговое электронное письмо полностью не соответствует целевой аудитории и что они прошли предварительное обучение, оповещения или предупреждения по вопросам фишинга.

После расчета окончательного рейтинга соответствия помещения его можно сопоставить с одной из трех категорий соответствия помещения.[4]:

- Сильная — суть фишингового письма сильно соответствует целевой аудитории, поэтому письмо трудно обнаружить как фишинговое.
- Средний – соответствие посыла фишингового письма целевой аудитории умеренное.
- Слабое — соответствие посыла фишингового письма целевой аудитории низкое, что делает письмо менее трудным для обнаружения фишинга.

Используйте сопоставление, представленное в таблице 6, чтобы определить категорию соответствия для фишингового электронного письма.

Таблица 6. Сопоставление категорий фишинговой электронной почты

Рейтинг выравнивания помещений	Категория планировки помещения
10 и ниже	Слабый
11 – 17	Середина
18 и выше	Сильный

Категория слабого, среднего или сильного выравнивания предпосылок переносится в раздел. 2.3, а также категорию сигналов из гл. 2.1.3.

[4] В Стивсе и др. В публикации [23] для выравнивания помещений использовались следующие категории: высокая, средняя и низкая. В этом руководстве пользователя будут использоваться термины сильный, средний и слабый. Хотя номинально категории различаются, их значение и категоризация остаются прежними.

2.3. Определение сложности обнаружения

Последним шагом в применении шкалы Фиша является определение общей сложности обнаружения электронного письма. Ранее определенные категории сигналов (см. раздел 2.1.3) и согласования предпосылок (см. раздел 2.2.3) для фишингового электронного письма анализируются коллективно, чтобы определить сложность обнаружения фишингового электронного письма, как показано в таблице 7.

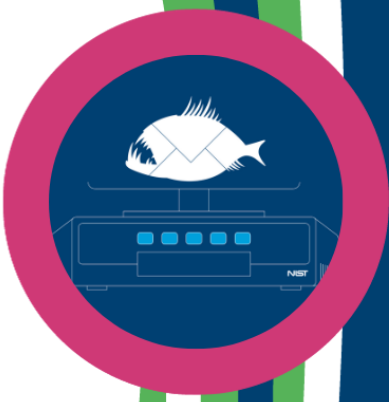
Таблица 7. Шкала Фиша – сложность обнаружения

Категория сигналов	Категория планировки помещения	Сложность обнаружения
Мало (сложнее)	Сильный	Очень сложно
	Середина	Очень сложно
	Слабый	Умеренно сложно
Некоторый	Сильный	Очень сложно
	Середина	Умеренно сложно
	Слабый	От умеренной до наименее сложной
Многие (менее сложные)	Сильный	Умеренно сложно
	Середина	Умеренно сложно
	Слабый	Наименее сложно

Электронные письма с небольшим количеством намеков и четким соответствием предпосылок человеку труднее обнаружить как фишинговые, чем письма с большим количеством намеков и слабым согласованием предпосылок.

Например, фишинговые электронные письма, отнесенные к категории «Несколько» намеков и «Средняя» направленность, имеют рейтинг сложности обнаружения «Очень сложно». Или фишинговые электронные письма, отнесенные к категории «Некоторые» признаки и «Средняя» предпосылка, имеют рейтинг сложности обнаружения «Умеренно сложно».

3. Interpreting Results



Использование шкалы фишинга для понимания сложности обнаружения фишинговых писем помогает специалистам по обучению осведомленности о фишинге двумя основными способами. Во-первых, шкала Фиша предоставляет информацию о частоте кликов обучающих сообщений и частоте отчетов для целевой аудитории. Например, фишинговые электронные письма, которые очень сложно обнаружить, по понятным причинам могут привести к высокому количеству кликов при использовании в имитации фишинга; Наименее сложные электронные письма, вероятно, могут привести к снижению количества кликов. Однако, когда фишинг дает неожиданные результаты (например, наименее сложное электронное письмо, которое приводит к высокому количеству кликов), это может указывать на то, что для целевой аудитории необходимо модифицированное или дополнительное обучение.

Во-вторых, шкала фишинга дает возможность охарактеризовать реальные угрозы фишинга, чтобы специалисты по обучению могли снизить риск безопасности своей организации, адаптируя обучение к типам угроз, с которыми сталкивается их организация, сохраняя при этом устойчивый уровень безопасности. Одним из преимуществ сильной и устойчивой системы безопасности является защита внутреннего и внешнего доверия. Надежная программа фишинга не должна быть застойным упражнением типа «поставьте галочку», а, скорее, развивающейся частью зрелой программы повышения осведомленности и обучения в области кибербезопасности, обеспечивающей зрелые, основанные на показателях результаты. Организациям необходимо адаптировать свою программу обучения кибербезопасности и осведомленности к своей уникальной среде, потребностям и требованиям сотрудников, сохраняя при этом миссию своей организации и устойчивость к рискам. Уровень безопасности, реализуемый организацией, должен быть соразмерен ее риску, а также целям и операциям организации. Другими словами, чем выше риск, с которым сталкивается организация, тем более высокий уровень безопасности она должна реализовать.

Наконец, программа повышения осведомленности и обучения в области кибербезопасности не является панацеей от всех болезней. Организации необходим многосторонний подход, учитывающий технологии, процессы и людей, чтобы выявлять, реагировать и сообщать о подозрительных фишинговых атаках. При применении как в домашней, так и в рабочей среде пользователя эта тактика может дать пользователям конкретные навыки и знания, которые помогут им лучше подготовиться к защите от потенциальных попыток фишинга, защищая как пользователя, так и его организацию.

References

[1] Алазаб, Мамун и Бродхерст, Родерик, Спам и преступная деятельность (2016). Тенденции и проблемы преступности и уголовного правосудия (Австралийский институт криминологии), № 52, Исследовательский документ RegNet № 2014/44. DOI: 10.2139/ssrn.2467423

[2] Алутайби А., Арден-Клоуз Э., Макэлани Дж., Стефанидис А., Фалп К. и Али Р. (октябрь 2019 г.). Как дизайн социальных сетей может вызвать страх пропустить что-то? В Proc. Международной конференции IEEE по системам, человеку и кибернетике (SMC) 2019 г. (стр. 3758-3765). IEEE.

[3] Барриентос Ф., Джейкобс Дж. и Докинз С. Масштабирование фишинга: продвижение шкалы фишинга NIST. В материалах HCII 2021 (23-я Международная конференция по взаимодействию человека и компьютера). 24 июля – 29 июля 2021 г. DOI: 10.1007/978-3-030-78642-7_52.

[4] Докинз С. и Джейкобс Дж. (2023). Как масштабировать фиш: исследование использования шкалы фишинга NIST. Материалы девятнадцатого симпозиума по полезной конфиденциальности и Безопасность, Анахайм, Калифорния, США.

[5] де Зафра Д., Питчер С., Тресслер Дж., Ипполито Дж. (1998). Требования к обучению безопасности информационных технологий: модель, основанная на ролях и производительности. (Национальный институт стандартов и технологий, Гейтерсбург, Мэриленд), Специальная публикация NIST (SP) 800-16. DOI: 10.6028/NIST.SP.800-16.

[6] Даунс Дж. С., Холбрук М. и Крейнор Л. Ф. (июль 2006 г.). Стратегии принятия решений и подверженность фишингу. В Proc. Второго симпозиума по полезной конфиденциальности и безопасности (SOUPS '06), ACM, 2006, стр. 79–90.

[7] Федеральный закон о модернизации информационной безопасности 2014 г., Публикация. Л. № 113-283 (2014). https://www.govinfo.gov/app/details/PLAW-113publ283 (последнее посещение: октябрь 2023 г.).

[8] Грациоли, С. (2004, март). Где они ошиблись? Анализ неспособности осведомленных интернет-потребителей обнаружить обман в Интернете. Групповое решение и переговоры 13, 149–172 (2004). DOI: 10.1023/B:GRUP.0000021839.04093.5d

[9] Грин К.К., Стивс М., Теофанос М. и Костик Дж. (2018). Пользовательский контекст: независимая переменная восприимчивости к фишингу. В Proc. семинара «Usable Security» (USEC) 2018 года на симпозиуме «Безопасность сетей и распределенных систем» (NDSS).

[10] Хаднаги К. и Финчер М. (2015). Темные воды фишинга: наступательная и защитная стороны вредоносных электронных писем. Уайли и сыновья.

[11] Центр рассмотрения жалоб на интернет-преступления (IC3), Федеральное бюро расследований. (2023). Отчет о преступности в Интернете за 2022 год.https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (Последний раз получено в октябре 2023 г.).

[12] Якобссон, М. (2007). Человеческий фактор в фишинге. Конфиденциальность и безопасность потребительской информации.

[13] Каракасилиотис А., Фурнелл С.М. и Пападаки М. (2006). Оценка осведомленности конечных пользователей о социальной инженерии и фишинге. В материалах 7-й австралийской конференции по информационной войне и безопасности, Университет Эдит Коуэн, Перт, Западная Австралия, 4-5 декабря 2006 г. DOI: 10.4225/75/57a80e47aa0cb

[14] Макэлани Дж. и Хиллз П.Дж. Понимание обработки фишинговой электронной почты и восприятие надежности посредством отслеживания глаз. Фронт Психол. 2020 28 июля;11:1756. DOI: 10.3389/fpsyg.2020.01756. PMID: 32849040; PMCID: PMC7399207.

[15] Молинаро, штат Калифорния (2019). Понимание фишинга: использование анализа суждений для оценки человеческого суждения о фишинговых электронных письмах (докторская диссертация, Государственный университет Нью-Йорка в Буффало).

[16] Национальный институт стандартов и технологий (2020 г.) Средства контроля безопасности и конфиденциальности для федеральных информационных систем и организаций. Специальная публикация 800-53, Ред. 5. DOI: 10.6028/NIST.SP.800-53r5.

[17] Ниелес М., Демпси К. и Пиллиттери В.Ю. (2017). Введение в информационную безопасность. (Национальный институт стандартов и технологий, Гейтерсбург, Мэриленд), Специальная публикация NIST (SP) 800-12, Ред. 1. DOI: 10.6028/NIST.SP.800-12r1

[18] О'Доннелл, Л. (май 2019 г.). Список угроз: 5 самых опасных типов прикреплений. https://threatpost.com/threatlist-top-5-most-dangerous-attachment-types/144635/ (Последний раз получено в октябре 2023 г.)

[19] Циркуляр А-130 Управления управления и бюджета, Управление информацией как стратегическим ресурсом, июль 2016 г. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a1_30revised.pdf (Последний раз получено в октябре 2023 г.).

[20] Парсонс, К., Бутавичиус, М., Паттинсон, М., Калич, Д., Маккормак, А., Джеррам, К. (2016). Фокусируются ли пользователи на правильных признаках, чтобы отличить фишинговые письма от подлинных?

[21] Парсонс К., МакКормак А., Паттинсон М., Бутавичиус М., Джеррам К. (2013). Фишинг в поисках правды: основанный на сценариях эксперимент по поведенческой реакции пользователей на электронные письма. В: Безопасность и защита конфиденциальности в системах обработки информации (SEC 2013). Достижения ИФИП в области информационных и коммуникационных технологий, том 405. Springer, Берлин, Гейдельберг. DOI: 10.1007/978-3-642-39218-4_27.

[22] Стивс М., Грин К. и Теофанос М. (2019). Шкала фишинга: оценка сложности обнаружения фишинговых сообщений человеком. В материалах семинара по полезной безопасности 2019 года. Сан-Диего, Калифорния. DOI: 10.14722/usec.2019.23028

[23] Стивс М., Грин К. и Теофанос М. (2020). Классификация сложности человеческого фишинга: шкала фишинга. Журнал Кибербезопасности, 6(1), tyaa009. DOI: 10.1093/cybsec/tyaa009

[24] Цоу А. и Якобссон М. (2007). Обман и обман: крупное пользовательское исследование фишинга.

[25] Уилсон М. и Хэш Дж. (2003). Создание программы повышения осведомленности и обучения безопасности информационных технологий. (Национальный институт стандартов и технологий, Гейтерсбург, Мэриленд), Специальная публикация NIST (SP) 800-50. DOI: 10.6028/NIST.SP.800-50

[26] Райт, Р.Т., Дженсен, М.Л., Тэтчер, Дж.Б., Динджер, М. и Маретт, К. (2014) Исследовательская записка — Методы воздействия при фишинговых атаках: исследование уязвимости и устойчивости. Исследования информационных систем 25(2):385-400. DOI: 10.1287/isre.2014.0522.

Appendix A: NIST Phish Scale Worksheet

Этот заполняемый рабочий лист можно использовать при применении шкалы фишинга NIST к фишинговому электронному письму. Рабочий лист состоит из трех частей: «Подсказки» (раздел A.1), «Выравнивание помещения» (раздел A.2) и «Трудность обнаружения» (раздел A.3).

A.1. Электронная почта

Форму ниже можно использовать для подсчета количества сигналов фишингового письма. Первая часть формы состоит из вопросов об электронном письме с ответами да/нет. Ответы на вопросы во второй части формы должны представлять собой общее количество экземпляров соответствующего сигнала, найденного в электронном письме. Эта сумма, добавленная к количеству ответов «да» в первой части формы, дает итоговое количество наблюдаемых сигналов для этого фишингового письма. Эта итоговая сумма затем используется для классификации фишинговых сигналов.

Часть 1. Ответьте «да» или «нет» на следующие вопросы:

Технические индикаторы

Не связано ли имя отправителя с адресом электронной почты отправителя, включая адрес для ответа?

Является ли доменное имя, используемое в адресе электронной почты отправителя, похожим на домен узнаваемого объекта?

Индикаторы визуального представления

Отсутствуют ли соответствующие элементы брендинга (текст или логотипы)?

Дизайн и форматирование электронного письма кажутся непрофессиональными?

Язык и содержание

В электронном письме отсутствует общее приветствие, например официальное или неофициальное приветствие?

В электронном письме отсутствует персонализация?

В сообщении отсутствуют сведения об отправителе, например отправитель или контактная информация?

Общая тактика

Похоже ли сообщение на рабочий или бизнес-процесс?

Похоже, что сообщение пришло от друга, коллеги, начальника, другого авторитетного лица или другого авторитетного лица?

Общее количество ответов «да»: 0

Часть 2. Подсчитайте общее количество раз, когда в электронном письме появляется следующее:

Ошибки

Сколько орфографических ошибок в письме? _____

Сколько грамматических ошибок в электронном письме, включая несовпадающее множество? Сколько несоответствий в письме? _____

Технические индикаторы

Сколько потенциально опасных вложений включено? Сколько раз текст скрывает настоящий URL-адрес в гиперссылке? _____

Сколько ссылок имеют доменное имя, правдоподобно похожее на домен узнаваемого объекта? _____

Индикаторы визуального представления

Сколько элементов брендинга (текста или логотипов) являются имитацией? _____

Сколько элементов брендинга (текста или логотипов) кажутся устаревшими? _____

Сколько недопустимых индикаторов безопасности или значков безопасности в электронном письме? _____

Язык и содержание

Сколько раз в сообщении используется юридический язык, например информация об авторских правах, отказ от ответственности или налоговая информация? _____

Сколько подробных аспектов, не являющихся центральными для содержания, содержится в сообщении? _____

Сколько запросов на конфиденциальную информацию содержится в электронном письме, включая личную информацию или учетные данные? _____

Сколько раз в электронном письме выражается нехватка времени, в том числе подразумеваемая? Сколько угроз содержится в сообщении, включая подразумеваемые угрозы? _____

Общая тактика

Сколько обращений содержится в электронном письме с просьбой помочь другим? _____

Сколько раз электронные письма предлагают что-то слишком хорошее, чтобы быть правдой, например, победу в конкурсе, лотерею, бесплатный отпуск и так далее? _____

Предлагает ли электронное письмо что-то персонализированное и неожиданное именно для вас? _____

Сколько раз электронное письмо предлагает что-то в течение ограниченного времени? _____

Сумма подсчитанных сигналов: 0

*Общее количество сигналов*из Части 1 (ответы «да») и Части 2 (подсчет сигналов): 0

The *общее количество сигналов*сопоставлен с соответствующей категорией в таблице 1 таблицы шкалы Фиша.

Таблица 1. Таблица 1. Сопоставление категорий сигналов

Общее количество сигналов	Категория сигнала
1–8 сигналов	Мало (сложнее)
9–14 реплик	Некоторый
15 и более реплик	Многие (менее сложные)

Категория реплики: _____

A.2. Выравнивание помещения

Этот рабочий лист можно использовать для расчета выравнивания помещения.

Для каждого элемента ниже присвойте оценку применимости в соответствии со шкалой применимости, приведенной в таблице 2 таблицы шкалы Фиша.

*1)**Имитирует процесс или практику на рабочем месте***

Насколько электронная почта применима к процессам или практикам на рабочем месте для целевой аудитории?

*2)**Имеет актуальность на рабочем месте***

Насколько идея электронного письма соответствует ролям и обязанностям целевой аудитории?

*3)**Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту.***

Насколько электронное письмо соответствует другим ситуациям или событиям, даже внешним по отношению к рабочему месту?

*4)**Вызывает беспокойство по поводу последствий НЕ нажатия***

Насколько применимо электронное письмо к опасениям по поводу потенциально вредных последствий для*нет*нажимаете на ссылки или вложения?

*5)**Был объектом целевого обучения, специальных предупреждений или иного воздействия.***

Насколько применимо отражение в электронном письме целевых обучающих эффектов, которые могут привести к обнаружению помещений? Необходимо позаботиться о том, чтобы надлежащим образом учесть специфику обучения или предупреждения, поскольку передача знаний довольно сложна.

Таблица 2. Таблица 2. Шкала применимости.

Шкала применимости	Оценка применимости
Экстремальная применимость, выравнивание или релевантность	8
Значительная применимость, выравнивание или релевантность	6
Умеренная применимость, выравнивание или релевантность	4
Низкая применимость, выравнивание или релевантность	2
Непригодный, нет выравнивания или нет релевантности	0

Сумма баллов применимости для элементов выравнивания помещения с 1 по 4 минус балл применимости для элемента согласования помещения 5 и есть ваш рейтинг согласования помещения.

Рейтинг выравнивания помещения: _____

Рейтинг выравнивания помещения сопоставляется с соответствующей категорией в таблице 3 таблицы шкалы Фиша.

Таблица 3. Таблица 3. Сопоставление категорий выравнивания помещений

Рейтинг выравнивания помещений	Категория планировки помещения
10 и ниже	Слабый
11 – 17	Середина
18 и выше	Сильный

Категория планировки помещения:_____

A.3. Сложность обнаружения

Категория сигнала и категория соответствия помещения используются для определения сложности обнаружения в соответствии с Таблицей 4 таблицы шкалы фишинга. Этот окончательный рейтинг сложности обнаружения следует использовать для контекстуализации частоты кликов и частоты отчетов в учебных упражнениях по предупреждению фишинга.

Таблица 4. Таблица 4. Шкала фишинга – сложность обнаружения

Категория сигналов	Категория планировки помещения	Сложность обнаружения
Мало (сложнее)	Сильный	Очень сложно
	Середина	Очень сложно
	Слабый	Умеренно сложно
Некоторый	Сильный	Очень сложно
	Середина	Умеренно сложно
	Слабый	От умеренной до наименее сложной
Многие (менее сложные)	Сильный	Умеренно сложно
	Середина	Умеренно сложно
	Слабый	Наименее сложно

Общий рейтинг сложности обнаружения: _____

Appendix B: Detailed Cues Descriptions

В этом приложении представлена дополнительная информация о сигналах и типах сигналов, включая примеры сигналов, сведения о том, где найти сигнал в сообщении электронной почты, а также ссылки в литературе.

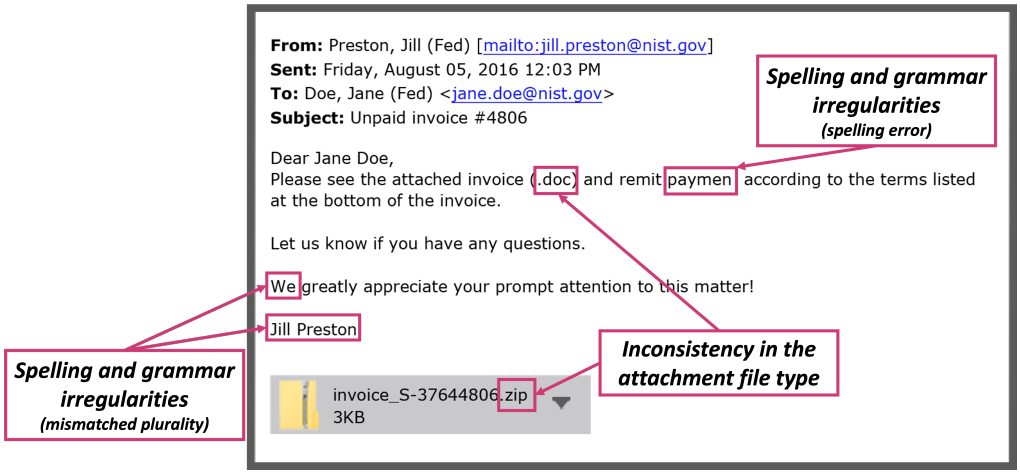
Б.1. Сигналы ошибок

Б.1.1. Орфографические и грамматические нарушения

> Обычно встречается в любой части электронного
>
> письма. Пример показан в Приложении В, Рисунок 1.
>
> Обратите внимание на любые грамматические ошибки, орфографические ошибки, ошибки пунктуации или несовпадающее множество в заголовках, теле и теме электронного письма (например, использование слова «комплимент» вместо «дополнение»). Несовпадающее множество возникает, если в тексте электронного письма используются местоимения во множественном числе (например, «мы»), но в строке подписи указано единственное лицо (например, от отдельного «Джон Доу»), или наоборот.
>
> *Ссылки: Парсонс и др., 2016 [20]; Каракасилиотис и др., 2006 г. [13]*

Б.1.2. непоследовательность

> Обычно встречается в любой части электронного
>
> письма. Пример показан в Приложении В, Рисунок 1.
>
> Непоследовательные сигналы — это элементы, которые могут показаться странными или неожиданными в нормальном электронном письме, но часто встречаются в фишинговых письмах. Несоответствия в сообщении электронной почты могут включать несоответствие типа вложения, отправленного и упомянутого в теле электронного письма, или подпись в теле электронного письма, которая не соответствует отправителю в строке «От».
>
> *Ссылки: Грациоли, 2004 г. [8]*



Приложение В Рис. 1. Пример электронного письма с сигналами о типе ошибки

Б.2.1. Тип прикрепления

Обычно находится во вложении к электронному письму.

Пример показан в Приложении В, Рисунок 2.

Любой тип вложения требует включения этого сигнала в счетчик сигналов, включая изображения (например, .jpeg), PDF-файлы (например, .pdf), исполняемые файлы (например, .exe) и сжатые файлы (например, .zip). .

Ссылки: Алазаб и Бродхерст, 2016 г. [1]; О'Доннелл, 2019 г. [18]

Б.2.2. Отображаемое имя и адрес электронной почты отправителя

Обычно находится в заголовке электронного письма.

Пример показан в Приложении В, Рисунок 2.

Засчитайте этот сигнал, если отображаемое имя отправителя не совпадает с адресом «От» и/или адресом «Ответить». Поддельное отображаемое имя может содержать надпись «IT Helpdesk», но адрес для ответа может быть « accounts-payable@gmail.com ». Убедитесь, что строка «from» в заголовке одинакова для этих двух элементов.

Ссылки: Парсонс и др. др., 2016 [20]; Каракасилиотис и др., 2006 [13]; Молинаро, 2019 г. [15]

Б.2.3. URL-гиперссылка

Обычно находится в теле сообщения или в постскриптуме электронного письма.

Пример показан в Приложении В, рис. 2.

Этот сигнал возникает, когда гиперссылка скрывает истинный URL-адрес за текстом, отформатированным либо как обычный текст, либо как другая ссылка. Примером может служить гиперссылка на www.nist.gov, которая в тексте неправильно отображается как «Министерство обороны».

Ссылки: Парсонс и др., 2016 [20]; Цоу и Якобссон, 2007 г. [24]; Каракасилиотис и др., 2006 г. [13]

Б.2.4. Подмена домена

Обычно находится в заголовке, теле сообщения или постскриптуме электронного письма.

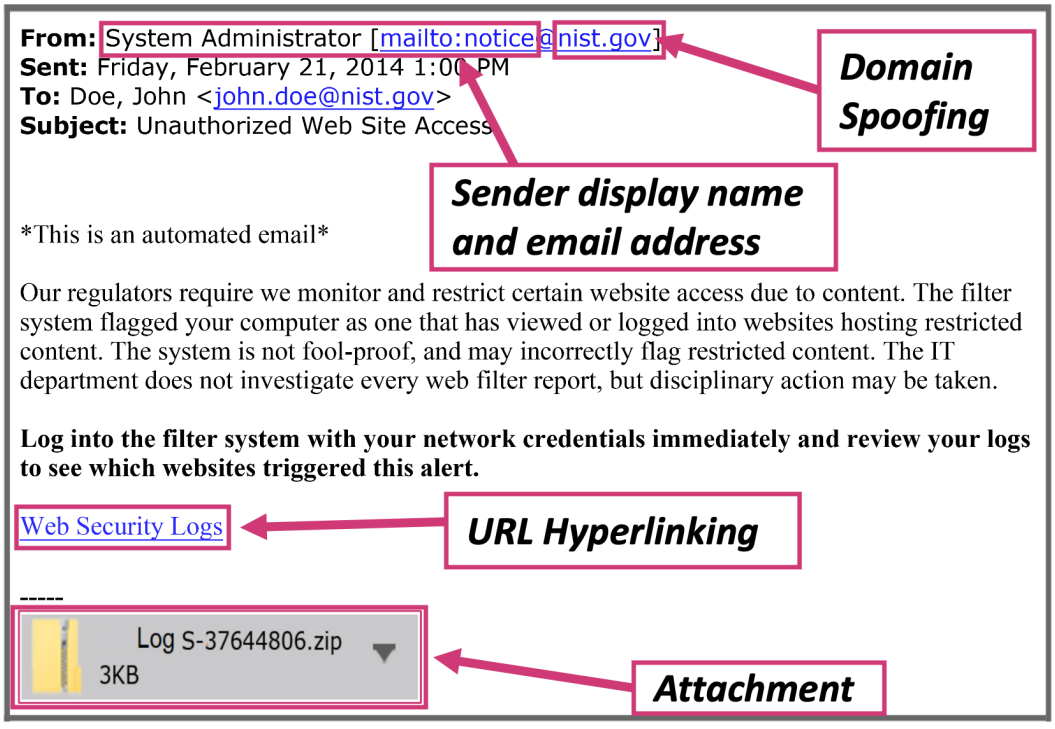
Пример показан в Приложении В, рис. 2.

Это признак того, что домен выглядит как принадлежащий веб-сайту, хорошо известному целевой аудитории. Чтобы учесть этот сигнал, доменное имя должно быть не просто правдоподобным; целевая аудитория должна узнавать его как знакомый и законный домен. Домен может выглядеть законным или очень напоминать законный домен. Этот сигнал можно посчитать несколькими способами, в том числе:

- Если заголовок содержит адрес электронной почты «От» с доменом, который выглядит заслуживающим доверия. Например, если отправителем был « jane.doe@nist.gov ».
- Если отображаемый текст гиперссылки в теле электронного письма имеет домен, который выглядит заслуживающим доверия. Например: «Пожалуйста, посетите https://www.ni-st.gov для получения дополнительной информации».
- Если URL-адрес гиперссылки в теле письма имеет домен, который выглядит заслуживающим доверия. Например, если при наведении курсора на текст отображается URL-адрес «https://www.nist.com».

Примечание. Не учитывайте этот сигнал, если URL-адрес и отображаемый текст совпадают, а также имеется ссылка на законный веб-сайт (например, www.nist.gov).

Ссылки: Каракасилиотис и др., 2006 [13]; Цоу и Якобссон, 2007 г. [24]



Приложение В Рисунок 2. Пример электронного письма с подсказками типов технических индикаторов

Б.3. Индикаторы визуального представления

Б.3.1. Брендинг и логотипы отсутствуют/минимальны

> Обычно находится в теме или сообщении электронной
>
> почты. Пример показан в Приложении В, рис. 3.
>
> Учтите этот сигнал, если какой-либо соответствующий брендинг отсутствует. Сюда могут входить отсутствующие логотипы, баннеры, текст и шрифты товарных знаков. Если электронное письмо обычно содержит брендинг или логотипы (например, от стороннего поставщика), учитывайте этот сигнал, если они отсутствуют; однако, если типичное электронное письмо не содержит брендинга (например, от коллеги), не учитывайте этот сигнал.
>
> *Ссылки: Каракасилиотис и др., 2006 [13]; Цоу и Якобссон, 2007 г. [24]*

Б.3.2. Имитация логотипа или устаревший брендинг/логотипы

> Обычно содержится в сообщении электронной
>
> почты. Пример показан в Приложении В, Рисунок 3.
>
> Учитывайте этот признак, если логотипы, баннеры или шрифты кажутся имитацией законных брендов/логотипов или являются устаревшими.
>
> *Ссылки: Каракасилиотис и др., 2006 [13]; Грин и др., 2018 г. [9]*

Б.3.3. Непрофессиональный дизайн или форматирование

> Обычно содержится в сообщении электронной
>
> почты. Пример показан в Приложении В, Рисунок 3.
>
> Учтите этот сигнал, если тело электронного письма выглядит непрофессионально, например, с разрывами строк в середине предложения, неуместным выделением, ненормальным форматированием текста или заголовков.
>
> *Ссылки: Каракасилиотис и др., 2006 [13]; Якобссон, 2007 г. [12]; Цоу и Якобссон, 2007 г. [24]*

Б.3.4. Индикаторы и значки безопасности

> Обычно содержится в сообщении электронной
>
> почты. Пример показан в Приложении В, Рисунок 3.
>
> Учтите, если в теле фишингового электронного письма виден значок замка, подтверждение безопасности, текст с цифровой подписью и т. д.
>
> *Ссылки: Цоу и Якобссон, 2007 г. [24]; Даунс и др., 2006 г. [6]*

Приложение B Рисунок 3. Пример электронного письма с подсказками типа индикатора визуального представления

Б.4. Языковые и контентные подсказки

Б.4.1. Юридический язык/информация об авторских правах/отказ от ответственности

> Обычно встречается в постскриптуме электронного письма.
>
> Пример показан в Приложении B, Рисунок 4.
>
> Учтите этот сигнал, если электронное письмо содержит текст, похожий на заявление об отказе от ответственности, включая предупреждения о безопасности или информацию о товарных знаках, авторских правах или другую юридическую информацию.
>
> Примечание. Не весь мелкий шрифт следует рассматривать как отказ от ответственности. *Ссылки: Якобссон, 2007 [12]; Цоу и Якобссон, 2007 г. [24]*

Б.4.2. Отвлекающие детали

> Обычно находится в теле сообщения электронной почты. Пример показан в Приложении B, рис. 4.
>
> Любой контент, не являющийся ключевым для цели электронного письма, может быть расценен как отвлекающая деталь. *Ссылки: Грин и др., 2018 г. [9]*

Б.4.3. Запросы конфиденциальной информации

> Обычно находится в теме или теле сообщения электронной почты.
>
> Пример показан в Приложении В, рис. 4.
>
> Учтите этот сигнал, если в электронном письме запрашивается такая информация, как личная информация (PII) или что-либо, напрямую связанное с финансами или личностью человека или организации (например, учетные данные для входа, номер социального страхования).
>
> *Ссылки: Даунс и др., 2006 [6].*

Б.4.4. В срочном порядке

> Обычно находится в теме или теле сообщения электронной почты.
>
> Пример показан в Приложении В, рис. 4.
>
> В теме письма или теле письма есть формулировка, указывающая на необходимость срочно заставить пользователей быстро выполнить требования. Этот сигнал включает в себя четкие сроки действий и более неявные формулировки (например, «немедленно»).
>
> *Ссылки: Парсонс и др., 2013 [21]; Макэлани и Хиллз, 2020 г. [14]; Райт и др., 2014 г. [26]*

Б.4.5. Угрожающий язык

> Обычно находится в теме или теле сообщения электронной почты.
>
> Пример показан в Приложении В, рис. 4.
>
> Учитывайте этот сигнал, если электронное письмо содержит угрозу из-за бездействия получателя. Угрозы могут быть личными, профессиональными, юридическими и т. д.
>
> *Ссылки: Каракасилиотис и др., 2006 [13].*

Б.4.6. Общее приветствие

> Обычно встречается в теме или сообщении электронной почты.
>
> Пример показан в Приложении В, рисунок 4.
>
> В электронном письме отсутствует персонализация (например, конкретное имя получателя) или какое-либо приветствие.
>
> *Ссылки: Парсонс и др., 2016 [20]; Якобссон, 2007 г. [12]; Каракасилиотис и др., 2006 [13]; Даунс и др., 2006 г. [6]*

Б.4.7. Отсутствие данных о подписанте

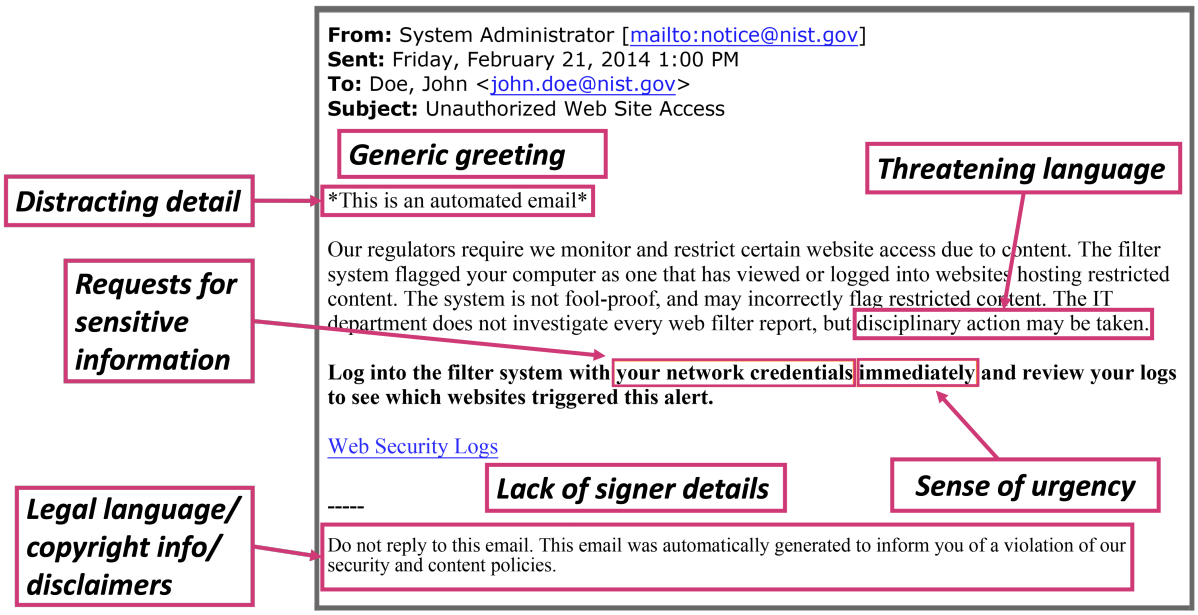
Обычно встречается в закрытии сообщения электронной

почты. Пример показан в Приложении В, рис. 4.

Засчитайте этот сигнал, если отсутствует что-либо из следующего:

- Подпись физического лица в теле письма.
- Контактная информация в теле письма. Это может быть должность отправителя, номер телефона, факс, адрес электронной почты или рабочий адрес.

Ссылки: Якобссон, 2007 г. [12]



Приложение В. Рис. 4. Пример электронного письма с указанием языка и типа контента.

Б.5. Общие тактические подсказки

Б.5.1. Гуманитарные обращения

Обычно находится в теме или теле сообщения электронной почты.

Пример показан в Приложении В, рис. 5.

Учтите этот сигнал, если электронное письмо фокусируется на желании получателя быть полезным, в том числе если предпринимаются попытки заручиться поддержкой благотворительного дела или аналогичных гуманитарных усилий.

Ссылки: Каракасилиотис и др., 2006 [13]; Алутайби и др., 2019 [2]; Хаднаги и Финчер, 2015 г. [10]

Б.5.2. Слишком хорошие, чтобы быть правдой предложения

> Обычно находится в теме или теле электронного письма.
>
> Пример показан в Приложении В, рис. 5.
>
> Электронное письмо предлагает получателю неожиданный или невероятный приз, например выигрыш в конкурсе или другие маловероятные денежные и/или материальные предложения.
>
> *Ссылки: Якобссон, 2007 [12]; Грациоли, 2004 г. [8]*

Б.5.3. Ты особенный

> Обычно находится в теме или теле сообщения электронной почты.
>
> Пример показан в Приложении В, рис. 5.
>
> В электронном письме есть формулировка, которая предполагает, что что-то особенное является неожиданным и предлагается только получателю (например, электронная открытка на День святого Валентина, специальный купон на день рождения). Этот сигнал предназначен не только для использования, когда получатель получает электронное письмо; его следует учитывать только тогда, когда предлагается что-то особенное.
>
> *Ссылки: Хаднаги и Финчер, 2015 г. [10]*

Б.5.4. Ограниченное по времени предложение

> Обычно находится в теме или теле сообщения электронной почты.
>
> Пример показан в Приложении В, рис. 5.
>
> Подобно сигналу «ощущение безотлагательности», этот сигнал следует учитывать, если в электронном письме указан четкий срок действия. Однако этот сигнал не следует считать типичным сигналом давления времени; его следует учитывать только в том случае, если содержание электронного письма что-то предлагает получателю.
>
> *Ссылки: Стивс и др., 2019 г.*

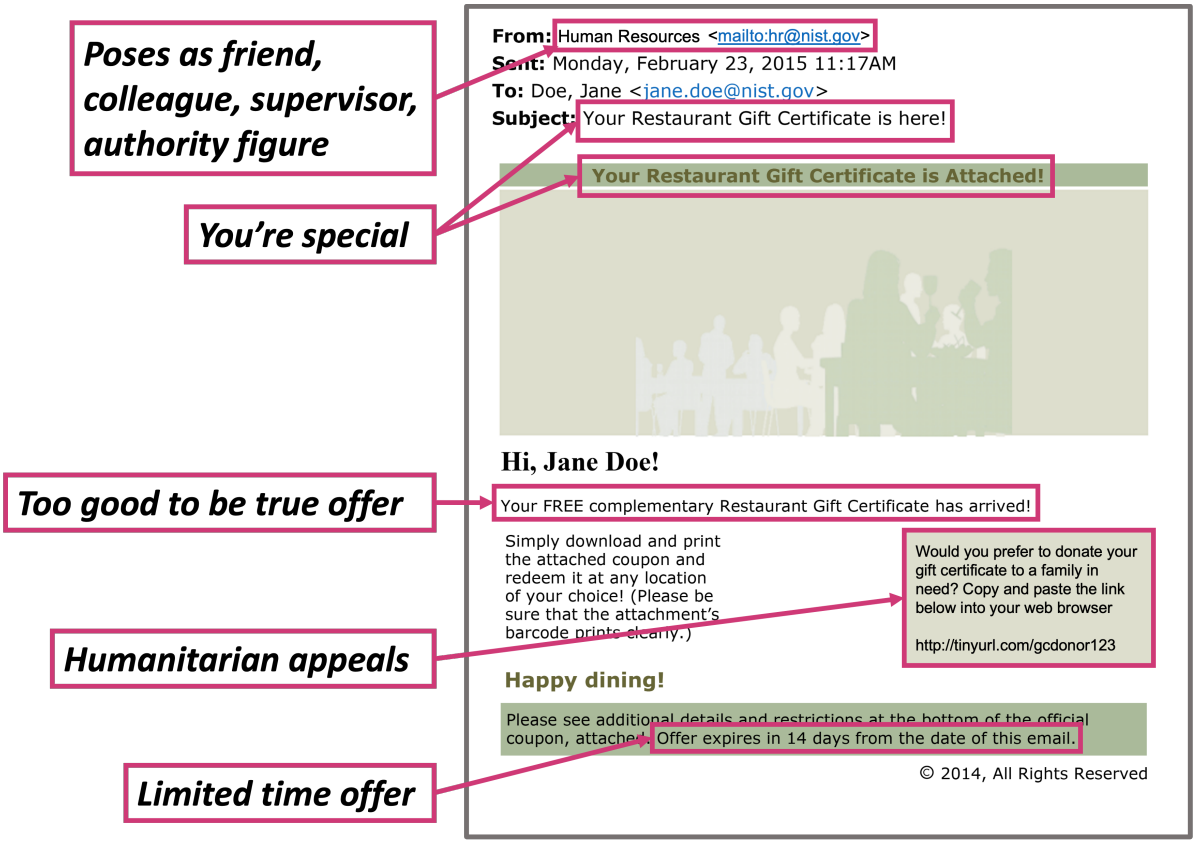
Б.5.5. Имитирует рабочий или бизнес-процесс

> Обычно находится в теме или сообщении электронной почты.
>
> Посылки писем в Приложении Б. Рисунки 1 и 2 являются примерами этого сигнала.
>
> Учитывайте этот сигнал, если электронное письмо связано с какой-либо практикой на рабочем месте или бизнес-операциями организации (например, уведомление голосовой почты, доставка посылок).
>
> *Ссылки: Стивс и др., 2019 г.*

Б.5.6. Выдает себя за друга, коллегу, начальника, авторитетную фигуру

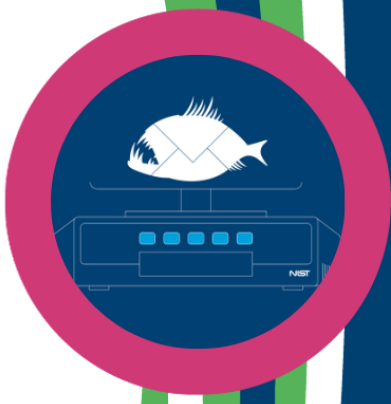
> Обычно находится в заголовке или закрытии сообщения электронной почты.
>
> Пример показан в Приложении В, рисунок 5.

> Этот сигнал можно найти в любом месте электронного письма, и он возникает всякий раз, когда отправитель отображается как человек, которому получатель может доверять (например, начальник, законная организация, семья и друзья).
>
> *Ссылки: Каракасилиотис и др., 2006 [13].*



Приложение B Рисунок 5. Пример электронного письма с подсказками типа Common Tactic

Appendix C: Glossary



Нажмите «Оценить»

Отношение количества людей, которые нажали на потенциально вредоносную ссылку или вложение в смоделированном фишинговом электронном письме, к общему числу людей, отправивших смоделированное фишинговое электронное письмо.

Сложность обнаружения

Трудность обнаружения человеческого фишинга является результатом применения к электронному письму шкалы фишинга NIST; это показатель того, насколько легко или сложно кому-либо обнаружить электронное письмо как фишинговое.

Кий

Наблюдаемые характеристики электронного письма, которые либо заставляют пользователя щелкнуть мошенническую ссылку или вложение, либо предупреждают пользователя о том, что электронное письмо может быть фишинговым.

Шкала Фиша NIST (Шкала Фиша)

Метод оценки сложности обнаружения человеком фишингового электронного письма.

Выравнивание помещения

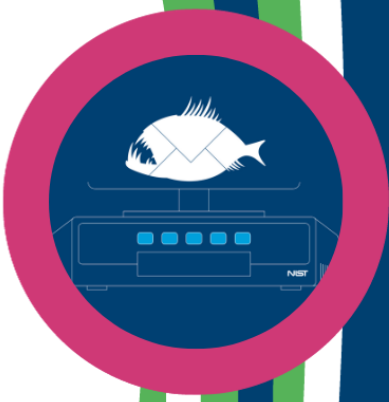
Применимость фишингового письма к целевой аудитории.

Целевая аудитория

Группа людей со схожей рабочей культурой или обязанностями, которым отправляется симулированное фишинговое электронное письмо.

Специалист по обучению

Организаторы обучения по повышению осведомленности о фишинге — это специалисты, использующие шкалу фишинга NIST, и обычно это специалисты по обучению осведомленности о кибербезопасности или другие специалисты по компьютерной безопасности, ответственные за проведение учебных занятий по фишингу.


NIST