**Статья со шкалой ФИША**

<https://academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453>

**Классификация сложности фишинга среди людей: шкала фишинга**

Мишель Стивс, Кристен Грин , Мария Феофанос

Журнал кибербезопасности , том 6, выпуск 1, 2020 г., tyaa009, https://doi.org/10.1093/cybsec/tyaa009

Опубликовано: 14 сентября 2020 г. История статьи

**Аннотация**

Поскольку организации продолжают вкладывать средства в программы обучения по повышению осведомленности о фишинге, многие директора по информационной безопасности (CISO) обеспокоены тем, что процент кликов по их учебным упражнениям высок или колеблется, поскольку они должны обосновывать бюджеты на обучение для должностных лиц организации, которые сомневаются в эффективности обучения по повышению осведомленности при кликах, ставки не снижаются. Мы утверждаем, что следует ожидать, что рейтинг кликов будет варьироваться в зависимости от сложности фишингового письма для целевой аудитории. Прошлые исследования показали, что, когда предпосылка фишингового электронного письма совпадает с рабочим контекстом пользователя, пользователям гораздо сложнее обнаружить фишинг. Учитывая это, мы предлагаем шкалу фишинга, чтобы директора по информационной безопасности и лица, занимающиеся обучением фишингу, могли легко оценить сложность своих фишинговых упражнений и помочь объяснить соответствующие показатели кликов. Мы основываем нашу шкалу на прошлых исследованиях признаков фишинга и пользовательского контекста и применяем шкалу к ранее опубликованным и новым данным, полученным в результате фишинговых операций на предприятиях. Шкала фишинга хорошо зарекомендовала себя с текущим набором данных о фишинге, но в будущем необходимо провести ее проверку с большим количеством фишинговых писем. Шкала фишинга показывает большие перспективы в качестве инструмента, помогающего организовать обмен данными о частоте кликов по фишинговым упражнениям в разных секторах.

**Введение**

Согласно официальному ежегодному отчету о киберпреступности Cybersecurity Ventures за 2019 год, к 2021 году ущерб от киберпреступлений будет стоить миру 6 триллионов долларов в год [1] . Эти прогнозы затрат подтверждаются историческими данными о киберпреступности и недавним годовым ростом. Кроме того, в отчете говорится о заметном увеличении хакерской деятельности, спонсируемой враждебными национальными государствами, а также деятельности организованных преступных синдикатов. Наконец, возможности для проведения кибератак, сумма уязвимостей, которые могут быть использованы для проведения атаки, продолжает расти, в значительной степени из-за стремительного развития устройств Интернета вещей (IoT). Люди являются еще одним особенно важным компонентом общей поверхности атаки, поскольку социальная инженерия продолжает оставаться успешной. Признавая важность человеческого поведения для кибербезопасности, организации все больше вкладывают средства в программы повышения осведомленности о кибербезопасности для своих пользователей компьютеров, уделяя особое внимание обучению фишингу. Встроенные курсы повышения осведомленности о фишинге популярны (а в некоторых случаях обязательны) в самых разных секторах, включая финансовые услуги, правительство, здравоохранение и научные круги. В этом типе обучения отправляются смоделированные фишинговые электронные письма, которые имитируют реальные угрозы, чтобы повысить осведомленность сотрудников о фишинге.

Много руководителей по информационной безопасности [1] (CISO) выразили обеспокоенность, что процент кликов по их тренировочным упражнениям высок. Это относится и к для более зрелым и долгосрочным программам повышения осведомленности, хотя директора по информационной безопасности часто ожидают, что прогрессивно снижающийся рейтинг кликов продемонстрирует эффективность обучения. Кроме того, окупаемость инвестиций (ROI) для такого обучения может быть поставлена ​​под сомнение, если процент кликов высок или даже изменчив. В то же время, низкий рейтинг кликов не обязательно указывает на эффективность обучения и вместо этого может означать, что использованные фишинговые электронные письма были: (i) слишком простыми, (ii) не релевантными контексту для большинства сотрудников, или (iii) фишинг повторялся или был очень похож на предыдущие упражнения. На самом деле, низкий рейтинг кликов и учебные программы в целом могут вызвать ложное чувство безопасности или самоуспокоенности, если рассматривать их отдельно. Рейтинг кликов программы обучения осведомленности о фишинге должен быть частью более комплексной программы [2].

Предыдущая работа [3] показала, что рейтинг кликов будет варьироваться в зависимости от контекстуальной релевантности фишинга, при этом высоко контекстуально релевантный фишинг приводит к резким скачкам рейтинга кликов, несмотря на годы обучения осведомленности о фишинге. Кроме того, злоумышленники продолжают уточнять и варьировать данные для фишинговых атак. Хотя «традиционные» фишинговые электронные письма, ориентированные на сбор учетных данных, по-прежнему весьма успешны, злоумышленники постоянно становятся все более изощренными и изобретательными, в том числе добавляют доставку вредоносных программ. Кроме того, существует много легкодоступной информации в Интернете, которую злоумышленники могут использовать, чтобы лучше адаптировать фишинг и извлечь выгоду из контекстуальной релевантности. В то время, как некоторая информация добровольно и открыто делится пользователями в социальных сетях, большая часть другой информации была раскрыта в результате крупномасштабных утечек данных [4].

В то время, как повторение важно для обучения распознаванию фишинга и формирования поведения при отправке сообщений, простое повторение одних и тех же или очень похожих фишинговых писем не отражает всего спектра фишинговых угроз, наблюдаемых в реальном мире. Важно соответствующим образом варьировать фишинговые упражнения и ставить перед персоналом задачи с контекстуально релевантными фишинговыми сообщениями разной сложности, чтобы они могли провести обучение новым видам мошенничества, для которых следует ожидать переменную частоту кликов. Это следует рассматривать не как отрицательный эффект, а скорее как положительный результат, поскольку это означает, что организации действительно обучают свой персонал фишинговым атакам, которые представляют текущие угрозы реального мира. Но как именно можно измерить сложность данного фишингового письма? Хотя мы можем измерить количество кликов апостериорно и сделать вывод о сложности обнаружения на основе этих цифр, мы бы предпочли априорный метод определения сложности. В обсуждениях с директорами по информационной безопасности на ежегодной конференции Healthcare CyberGard [5], Советом по информационной безопасности и конфиденциальности [6] и другими организациями, мы обнаружили, что метод определения сложности фишинговых сообщений действительно будет очень полезен для тех, кто отвечает за реализацию фишингового обучения. Чтобы удовлетворить эту потребность, мы предлагаем шкалу фишинга, простой способ для директоров по информационной безопасности и обучающих специалистов по внедрению, характеризовать сложность их фишинговых мероприятий и предоставить процедуру для определения соответствующих показателей. Эта процедура является пока отсутствующим элементом, который необходим специалистам по обучению, чтобы повысить пользу от тренировок и последующую рентабельность инвестиций.

В этой статье мы описываем наши исследовательские усилия по созданию предварительной концептуальной версии шкалы Фиша и ее компонентов. Кроме того, мы используем шкалу фишинга, чтобы определить рейтинг сложности для каждого из десяти подробно описанных упражнений по обучению фишингу из реального мира. Затем мы наблюдаем, соответствует ли оценка сложности каждого упражнения по шкале Фиша фактической частоте кликов по упражнению. Наконец, мы обсуждаем наши наблюдения, эффективность усилий на сегодняшний день, а также будущую работу, включая уточнение ее компонентов и проверку общего масштаба с помощью более широкого спектра фишинговых писем.

**Фон**

Для борьбы с фишингом электронной почты используются технологические и ориентированные на человека подходы. Подходы, ориентированные на технологии, включают такие механизмы, как фильтрация, брандмауэры и черные списки, тогда как подходы, ориентированные на человека, как правило, сосредоточены на обучении осведомленности о кибербезопасности и, часто, конкретно на фишинге. Отчасти благодаря достижениям в области машинного обучения (МО) и искусственного интеллекта (ИИ), фильтры электронной почты, в частности, становятся все более эффективными в блокировании общего спама. Это означает, что пользователи теперь видят меньше писем такого рода в своих почтовых ящиках. Недавняя работа постулировала существование «парадокса распространенности» [7], предполагая, что пользователи могут быть более уязвимы, когда такие электронные письма доходят, из-за их ограниченного опыта работы с потенциально вредоносными электронными письмами. Еще одна работа Леварии др. [8] показала, что люди часто расширяют свое представление о данном стимуле в ответ на уменьшение распространенности указанного стимула, например, рассматривая нейтральные лица как угрожающие, когда угрожающие лица стали редки.

Хотя серия экспериментов Levari et al. не занимались фишингом конкретно, учитывая набор тем, которые они исследовали, было бы правдоподобно ожидать, что их выводы будут относиться к области фишинга. Мы надеемся, что дополнительные исследования влияния распространенности на обнаружение фишинга — как для людей, так и для ИИ — позволят согласовать различные выводы о распространенности.

Помимо распространенности, существует множество других факторов, усложняющих обнаружение фишинговых писем человеком. Существует несколько существующих теорий и моделей восприимчивости к фишингу, которые очень важны для разработки шкалы фишинга. Эти теории и модели напрямую касаются типов сигналов электронной почты, тактики и индивидуальных характеристик пользователей, которые вместе помогают — по крайней мере частично — объяснить относительную простоту или сложность обнаружения фишинга людьми.

Теория мотивации защиты или PMT [9] рассматривала восприятие пользователями угрозы и соответствующую воспринимаемую способность управления угрозами. PMT в основном применялся к поведению безопасности в целом, хотя Wang et al. [10] применили PMT специально к восприятию угрозы фишинга. Гораздо позже, чем PMT, первоначально предложенная в 1975 году, была предложена Интегрированная модель обработки информации о восприимчивости к фишингу, или IIPM [11]. IIPM предполагает, что ограниченные ресурсы внимания пользователей для обработки информации, по существу, захватываются, когда определенные методы, такие как срочность, используются для влияния на поведение, а это означает, что пользователи полагаются на эвристическую обработку информации (Система I [12])), а не заниматься более глубокой и систематической обработкой (Система II [12]). Когда используется этот тип поверхностного стиля обработки информации, пользователи с большей вероятностью упускают из виду или игнорируют сигналы, которые в противном случае могли бы сообщить пользователю о законности электронного письма, например, неверный адрес отправителя. В 2016 году Вишванат и др. предложил модель подозрения, познания и автоматизма, или SCAM, в которой утверждалось, что индивидуальные характеристики пользователя вызывают вариативность в использовании эвристических процессов для оценки электронной почты [ 13 ].

В недавней работе Уильямса, Хиндса и Джойнсона [ 14 ] эти три модели (PMT, IIPM и SCAM) рассматривались в контексте работы международной организации с сайтами в Великобритании. В дополнение к типам моделей или теорий, таким как PMT, IIPM, SCAM, существует большое количество предыдущих работ, посвященных изучению или описанию влияния конкретных параметров электронной почты, таких как включение авторитетных сигналов и сигналов срочности. Исследование сигналов фишинга особенно важно для разработки шкалы фишинга, поскольку пользователи электронной почты полагаются на сигналы, чтобы определить, является ли конкретное сообщение электронной почты фишинговым.

Действительно, советы по борьбе с фишингом и обучение подчеркивают характеристики фишинговых сообщений, на которые должны обращать внимание пользователи электронной почты; их часто называют репликами, индикаторами и крючками. Список сигналов длинный и разнообразный, например, содержащийся в ссылках [ 15 , 16 ]. Поскольку не существует установленного шаблона того, какие подсказки могут содержаться в том или ином конкретном сообщении, задача для пользователей при определении того, является ли сообщение фишинговым, сложнее, чем если бы список был очень коротким. Еще более усложняя задачу, предшествующая работа показывает, что соответствие предпосылок фишинга и пользовательского контекста влияет на то, какие сигналы пользователь считает важными. Кроме того, один и тот же сигнал может быть привлекательным для одних пользователей, но вызывать подозрение у других — в зависимости от личности пользователя [2,3].

В. Грином и соавторами [3] данные об упражнениях по фишингу собирались в течение 4,5 лет в экологически приемлемом рабочем месте с соответствующими данными опроса за последний год. Исследование показало, что личность пользователя и его функционал чрезвычайно важны для восприимчивости к фишингу. Авторы предположили, что это была линза, через которую пользователи просматривали и интерпретировали сигналы электронной почты. Когда рабочий контекст пользователя не соответствовал предпосылке фишингового электронного письма, он с большей вероятностью обращал внимание на подозрительные сигналы, например, у них не было обязанностей по выставлению счетов на работе, а фишинговое электронное письмо якобы было неоплаченным счетом. Напротив, когда рабочий контекст пользователя был хорошо увязан с предпосылкой фишинговой электронной почты, они с большей вероятностью обращали внимание на убедительные сигналы и полностью игнорировали или в значительной степени не принимали во внимание подозрительные сигналы. В таком случае, Грин и др . [3] подчеркнули важность исследования фишинга на рабочем месте, поскольку большая часть предшествующей работы по фишингу проводилась в лабораториях с искусственным пользовательским контекстом или в университетских условиях, которые могут сильно отличаться от рабочего места. Уильямс и др [14] также рассмотрели эту потребность в данных о рабочем месте в своем исследовании.

Одно из немногих других исследований на рабочем месте было проведено Caputo et al [17], но из-за ограничений он смог только предположить важность пользовательского контекста. Мы также вносим свой вклад в растущий объем исследований фишинга на рабочем месте, применяя нашу шкалу фишинга к трем ранее опубликованным упражнениям по фишингу на рабочем месте в исх. [3], четыре упражнения по фишингу, подробно описанные в работе [18], а также составление отчетов и применение шкалы фишинга к данным трех ранее неопубликованных фишинговых операций на рабочем месте. Восемь из десяти упражнений имеют n's ∼70 для каждого упражнения, в то время как два из наших упражнений имеют намного большие размеры выборки, с n's ∼5000 для каждого упражнения.

**Метод**

Чтобы помочь организациям, которым поручено реализовать обучающие программы по борьбе с фишингом, важно учитывать относительную сложность обнаружения обучающих сообщений. Фишинговые сообщения, предназначенные для обучения или реальных угроз, могут быть более или менее сложными для данной рабочей группы. детектировать как попытку фишинга. Понимание сложности обнаружения помогает специалистам по обучению осведомленности о фишинге двумя основными способами: (i) предоставляя контекст, касающийся кликов обучающих сообщений и частоты сообщений для целевой аудитории, и (ii) предоставляя способ характеризовать фактические фишинговые угрозы, чтобы специалист по обучению мог снизить риск безопасности организации, адаптируя обучение к типам угроз, с которыми сталкивается их организация.

С этой целью мы разработали шкалу фишинга, чтобы помочь практикам оценить сложность обнаружения как обучающих, так и фактических фишинговых сообщений об угрозах. Шкала фишинга предназначена для классификации частоты кликов для встроенного обучения осведомленности о фишинге, а также для адаптации усилий по обучению. Мы ожидаем, что это предоставит директорам по информационной безопасности еще одну метрику, которая поможет оценить прогресс их программ повышения осведомленности с течением времени и устранить риски. Шкала предназначена для категоризации сложности обнаружения фишинговых сообщений по отношению к целевой аудитории.

В этом разделе мы опишем Phish Scale и операционализацию его компонентов в единой структуре. В следующем разделе мы представляем данные десяти обучающих упражнений по борьбе с фишингом на рабочем месте, чтобы проиллюстрировать, как получить рейтинг сложности фишинга с помощью шкалы фишинга.

**Шкала Фиша**

Чтобы разработать шкалу фишинга, мы начали с рассмотрения основных элементов, которые руководители по информационной безопасности и специалисты по обучению используют при выборе и настройке учебных упражнений по фишингу. Этими элементами являются предпосылка сценария и содержание сообщения. Предпосылка сценария может относиться к относительно новой угрозе или к более старой угрозе, которая остается эффективной для конкретной целевой аудитории. Содержание сообщения обычно настраивается инструктором и содержит подсказки, которые учащиеся могут использовать для обнаружения обучающего фишинга. Для этой исследовательской работы мы основываем шкалу фишинга на этих двух основных элементах: репликах, содержащихся в сообщении, и предпосылке, ориентированной на целевую аудиторию.

Другие факторы, такие как личность, любопытство, рассеянность, забота о безопасности и т. п., безусловно, влияют на количество кликов, и, в конечном счете, мы намерены рассмотреть, как учитывать дополнительные факторы, такие как эти; мы вернемся к этой теме в разделе будущих работ. Однако на данный момент эти усилия начинаются с подсказок сообщений и согласования предпосылок, поскольку эти элементы, несомненно, играют решающую роль в обнаружении фишинга людьми и, что важно, их можно классифицировать путем обучения разработчиков для данной целевой аудитории. Для этой первоначальной попытки охарактеризовать сложность обнаружения компоненты Phish Scale:

Система рейтинга наблюдаемых характеристик самого фишингового письма, таких как количество сигналов, характер сигналов, повторение сигналов и т. д.

Рейтинговая система для выравнивания предпосылки фишинговой электронной почты по отношению к целевой аудитории.

В таблице 1 представлена ​​наша исследовательская концептуальная структура, иллюстрирующая, как определяется рейтинг сложности обнаружения после определения категорий количества сигналов и выравнивания предпосылок. Пытаясь сохранить относительно простую категоризацию для обучения разработчиков, мы использовали три категории для каждого компонента и присваивали метки, представляющие относительные диапазоны для каждого. Вкратце, три категории, используемые для отражения эффекта «подсказок», содержащихся в фишинговом сообщении, включают несколько (меньшее число означает меньше возможностей для обнаружения), некоторые (умеренное количество подсказок) и много (большее количество подсказок, больше возможностей для обнаружения). возможности обнаружения). Точно так же три категории используются для характеристики выравнивания предпосылок; они высокие, средние,и низкий . Мы обсудим компоненты шкалы более подробно в следующих разделах после нескольких замечаний о концептуальной основе.

**Таблица 1**

Шкала Фиша

| **Количество сигналов** | **Выравнивание помещения** | **Сложность обнаружения** |
| --- | --- | --- |
| Несколько (сложнее) | Высокая | Очень сложно |
| Середина | Очень сложно |
| Низкий | Умеренно сложный |
| Немного | Высокая | Очень сложно |
| Середина | Умеренно сложный |
| Низкий | Умеренно или наименее сложно |
| Много (менее сложно) | Высокая | Умеренно сложный |
| Середина | Умеренно сложный |
| Низкий | Наименее сложный |

В концептуальной структуре мы признаем более сильное влияние компонента выравнивания предпосылок на сигналы; это согласуется с выводами, представленными в исх. [3]. Более сильное влияние выравнивания предпосылок отражается в рейтинге сложности обнаружения, который имеет тенденцию быть на очень сложном или среднем уровне сложности , когда выравнивание предпосылок классифицируется как Высокое или Среднее . Кроме того, во всей концептуальной структуре шкалы Phish имеется больше заданий с рейтингом сложности очень сложного обнаружения, чем заданий с наименьшей сложностью .

Оценка сложности обнаружения для комбинации «Некоторые подсказки» и « Низкое выравнивание предпосылок» оценивалась в диапазоне от « Умеренно» до «Наименее сложно» , что еще больше отражает наше убеждение в том, что даже « Низкое выравнивание предпосылок» может иметь непропорциональное влияние на увеличение сложности обнаружения. Хотя мы ожидаем, что все рейтинги будут основаны на эмпирических данных, это особенно верно для этой конкретной комбинации (низкое выравнивание предпосылок и некоторые сигналы). Наконец, мы намеренно не помечаем категорию как «Легко обнаружить» или аналогичную, поскольку ожидаем, что предпосылка любого фишингового сообщения, как правило, совпадает по крайней мере с несколькими пользователями , и для них обнаружение часто бывает непростым.

В конечном счете, мы ожидаем, что каждый рейтинг сложности обнаружения будет соответствовать диапазону показателей кликов. Например, можно ожидать, что обучающие фишинговые сообщения, которые имеют соответствующий рейтинг сложности обнаружения « наименее трудный», будут иметь процент кликов менее 10%. Вернемся к этой теме в обсуждении.

Далее мы обсудим операционализацию каждого компонента шкалы. В следующем разделе мы рассмотрим сопоставление реальных данных учебных упражнений по фишингу с этими концептуальными категориями и обсудим наши наблюдения.

Сигналы фишинговых сообщений

Чтобы включить в шкалу влияние подсказок фишинговых сообщений, мы решили использовать количество экземпляров тех характеристик, которые присутствуют в оцениваемом сообщении. Мы рассуждаем так: чем меньше признаков фишинга присутствует в сообщении, тем сложнее его обнаружить. И наоборот, чем больше признаков присутствует, тем больше у пользователя возможностей заметить наводку, вызывающую подозрения. Мы понимаем, что эффект от любого отдельного сигнала или крючка может различаться от случая к случаю и от человека к человеку. Действительно, мы возвращаемся к этой теме в дискуссии. В настоящее время в структуре есть три категории для описания количества этих характеристик: Мало (меньше возможностей для обнаружения). Некоторые и Много (больше возможностей для обнаружения).

Прежде чем мы сможем подсчитать подсказки, нам нужно определить, какие фишинговые характеристики — список подсказок, индикаторов и крючков — подходят для включения в структуру. Из исх. [3] мы видим, что конкретная фишинговая характеристика может либо вызывать подозрения (наводка), либо убедить (крючок), в зависимости от контекста пользователя. В соответствии с предшествующей литературой мы используем термин «сигнал». Однако мы понимаем это в более широком смысле характеристики фишингового сообщения. Мы требуем, чтобы каждый сигнал, включенный в структуру, мог быть привязан к объективно наблюдаемой характеристике сообщения.

Из литературы мы рассмотрели сборники фишинговых сигналов в ссылках [15] и [16]. Мы использовали сигналы, данные в исх. [15] в качестве отправной точки. Кроме того, мы изменили категории, пытаясь упорядочить сигналы от тех, которые часто вызывают подозрения, таких как ошибки, к тем, которые обычно убедительны, например, к обычным тактикам, причем эти тактики широко используются, потому что они по-прежнему убедительны. Это в лучшем случае грубый порядок категорий, но мы посчитали, что он лучше подходит для подсчета сигналов, чем приведенный в ссылках [15] и [16]. Категории следующие:

*Error* — относящиеся к орфографическим и грамматическим ошибкам и несоответствиям, содержащимся в сообщении;

*Технический индикатор* — относящийся к адресам электронной почты, гиперссылкам и вложениям;

*Индикатор визуального представления* — относящийся к брендингу, логотипам, дизайну и форматированию;

*Язык и содержание* — например, стандартное приветствие и отсутствие сведений об отправителе, использование цейтнота и угроз;

*Общая тактика* — использование гуманитарных призывов, слишком хороших, чтобы быть правдой предложений, ограниченных по времени предложений, изображать из себя друга, коллегу или авторитетную фигуру и так далее. Помимо подсказок и характеристик, приведенных в [15], мы добавили дополнительные фишинговые характеристики из ссылок [3, 16] и многих других.

В таблице 2 представлен список выявленных нами признаков, которые объективно присутствуют в фишинговых сообщениях. Кроме того, он также содержит краткое описание каждого, связанных с ним ссылок и критериев, которые мы использовали при принятии решения о том, присутствует ли конкретный сигнал в отдельном сообщении. Чтобы определить количество реплик, используйте критерии для каждой реплики, подсчитайте количество экземпляров для каждой и просуммируйте их.

**Таблица 2:**

оперативные подсказки фишинговых сообщений

| **Тип сигнала** | **Название сигнала** | **Описание** | **использованная литература** | **Критерии подсчета** |
| --- | --- | --- | --- | --- |
| Ошибка | Орфографические и грамматические нарушения | Орфографические или грамматические ошибки, несовпадение множественного числа и т. д. | [11, 19–30] | Содержит ли сообщение орфографические или грамматические ошибки, в том числе несовпадающее множественное число? |
| непоследовательность | Несогласованный контент в электронном письме | [3] | Есть ли несоответствия, содержащиеся в сообщении электронной почты? |
| Технический индикатор | Тип вложения | Наличие файловых вложений, особенно исполняемого файла | [31] | Есть ли потенциально опасное вложение привязанность? |
| Отображаемое имя отправителя и адрес электронной почты | Поддельные отображаемые имена — скрывает адреса отправителя и адреса электронной почты для ответа. | [11, 13, 19, 21, 22, 24, 27, 29, 32] | Скрывает ли отображаемое имя настоящего отправителя? |
| гиперссылка URL | Гиперссылка URL-адреса скрывает истинный URL-адрес за текстом; текст также может выглядеть как другая ссылка | [20–22, 25, 27, 33] | Есть ли текст, который скрывает истинный URL-адрес в гиперссылке? |
| Подмена домена | Доменное имя, используемое в адресе электронной почты и ссылках, выглядит правдоподобно | [3, 34] | Действительно ли доменное имя, используемое в адресах или ссылках, похоже на домен законного лица? |
| Индикатор визуального представления | Отсутствие/минимум брендинга и логотипов | Нет или минимальное количество брендинга и логотипов | [13, 19, 22, 23, 25, 27, 32, 34, 42] | Отсутствует соответствующий брендинг? |
| Имитация логотипа или устаревший бренд/логотип | Подделка или имитация логотипа/устаревшего логотипа | [3, 24] | Какие-либо элементы брендинга кажутся имитацией или устаревшими? |
| Непрофессионально выглядящий дизайн или форматирование | Элементы форматирования и дизайна, которые не были созданы профессионально | [25, 27, 28, 34–36] | Нарушают ли дизайн и форматирование какую-либо общепринятую профессиональную практику? |
| Индикаторы безопасности и значки | Индикаторы безопасности и значки | [ 25, 35] | Имеются ли какие-либо неподходящие индикаторы безопасности или значки? |
| Язык и содержание | Юридический язык/информация об авторских правах/отказ от ответственности | Любой юридический язык, такой как информация об авторских правах, отказ от ответственности, налоговые последствия | [ 25] | Содержит ли сообщение какие-либо юридические формулировки, такие как информация об авторских правах, отказ от ответственности, налоговая информация? |
| Отвлекающие детали | Отвлекающие детали | [ 3 ] | Содержит ли сообщение какие-либо подробные аспекты, не являющиеся центральными для содержания? |
| Запросы конфиденциальной информации | Запросы конфиденциальной информации, такой как номер социального страхования или другая идентифицирующая информация. | [3, 21, 22] | Содержит ли сообщение запрос на предоставление какой-либо конфиденциальной информации, включая личную информацию или учетные данные? |
| В срочном порядке | Использование цейтнота, чтобы попытаться заставить пользователей быстро выполнить запрос. | [11, 20–22, 24, 27, 32, 37] | Содержит ли сообщение цейтнот, в том числе подразумеваемый? |
| Угрожающий язык | Использование угроз, таких как юридические разветвления | [11, 20, 21, 27, 32, 37] | Содержит ли сообщение угрозу, в том числе подразумеваемую угрозу? |
| Общее приветствие | Общее приветствие и полное отсутствие персонализации в электронном письме. | [20, 21, 24, 27, 28, 33, 34, 37] | В сообщении отсутствует приветствие или отсутствует персонализация в сообщении? |
| Отсутствие данных о подписавшемся | Электронные письма, содержащие несколько сведений об отправителе, например контактную информацию. | [24, 32] | В сообщении отсутствуют сведения об отправителе, например контактная информация? |
| Общая тактика | Гуманитарные призывы | Призывы помочь нуждающимся | [24, 27, 32] | Содержится ли в сообщении призыв помочь другим? |
| Слишком хорошие, чтобы быть правдой предложения | Выигрыши в конкурсах или другие маловероятные денежные и/или материальные предложения | [23, 24, 27, 28, 30] | Предлагает ли сообщение что-то слишком хорошее, чтобы быть правдой, например, выигрыш в конкурсе, лотерею, бесплатный отпуск и так далее? |
| Ты особенный | Специально для вас предлагаю… например, электронную открытку-валентинку от тайного поклонника | [24] | Сообщение предлагает что-нибудь только для вас? |
| Ограниченное по времени предложение | Это предложение продлится недолго… | [24] | Предлагает ли сообщение что-либо в течение ограниченного времени? |
| Имитирует рабочий или бизнес-процесс — законное электронное письмо | Имитирует любой правдоподобный рабочий процесс, такой как новая голосовая почта, доставка посылки, подтверждение заказа, уведомление о счете и т. д. | [24] | Представляется ли сообщение рабочим или бизнес-процессом? |
| Выдает себя за друга, коллегу, начальника, авторитетную фигуру | Электронное письмо якобы от друга, коллеги, начальника или другого авторитетного лица | [14, 24] | Похоже, что сообщение от друга, коллеги, начальника или другого авторитетного лица? |

Мы признаем, что для этих первоначальных усилий этот список не является исчерпывающим и будет расширяться. Кроме того, мы ожидаем, что некоторая форма взвешивания может быть полезна для отражения важности сигнала. Однако, учитывая изменчивость значимости сигналов для отдельных лиц в целевой популяции, это нетривиальное упражнение. Мы ожидаем, что такие уточнения будут тщательно изучены при дальнейшем развитии шкалы.

Для целей шкалы фишинга мы не включали подсказки фишинговых сообщений, связанные с несоответствиями с миром пользователя, такими как конкретные рабочие обязанности человека или ожидания человека, например, ожидание важного телефонного звонка. Рабочие обязанности и общие ожидания целевой аудитории на рабочем месте объединены в компонент согласования предпосылок шкалы Phish, описанный далее.

**Выравнивание помещения для фишинга**

Включение выравнивания посылок — это процесс определения уместности отправки сообщения электронной почты для целевой аудитории. Он пытается зафиксировать согласованность со следующим для целевой аудитории: правдоподобие рабочих обязанностей и деловой практики, уместность темы на рабочем месте, соответствие другим событиям или ситуациям, в том числе внешним по отношению к рабочему месту, озабоченность тем, чтобы не щелкнуть мышью, и разоблачение или предупреждения о предпосылка, которая повлияет на склонность кликать. Еще один способ увидеть соответствие — это то, что делает предпосылку убедительной. В целом, мы пытаемся классифицировать выравнивание предпосылок, а не несоответствие предпосылок, которые в некотором смысле противоположны друг другу. Несмотря на это, мы признаем смягчающее влияние обучения и осведомленности на распознавание фишинга и считаем, что это следует учитывать при классификации предпосылок. Особенно хорошим примером этого смягчающего эффекта является широкое распространение информации о нигерийской афере 419 [24], которая настолько хорошо известна, что многие ее разновидности обычно признаются мошенническими.

Мы ожидаем, что согласование предпосылок будет определять специалист по обучению конкретному фишинговому сообщению — кто-то, кто знаком с культурой работы целевой аудитории, обязанностями и ожиданиями как группы. Выравнивание предпосылок не может быть определено абстрактно; знание контекста работы целевой аудитории в отношении предпосылки фишингового сообщения имеет решающее значение для точной классификации предпосылок. Мы используем три категории для характеристики выравнивания: высокое, среднее и низкое. Чтобы определить соответствие предпосылкам, организатор обучения должен понять и классифицировать соответствие предпосылок для целевой аудитории. Мы разработали два метода категоризации выравнивания предпосылок. Один использует смешанную перспективу, а второй использует шаблонный подход к категоризации выравнивания предпосылок. Метод смешанной перспективы использует три рейтинга: высокий, средний и низкий, чтобы классифицировать, насколько сильно предпосылка согласуется с частями целевой аудитории в широком смысле, а затем объединяет их в общий рейтинг. Формульный подход состоит из пяти элементов, каждый из которых оценивается, а затем оценки суммируются для получения общей оценки. Тот или иной метод может больше понравиться отдельным разработчикам обучения; мы описываем оба.

**Метод 1: Категоризация выравнивания помещения со смешанной перспективой**

Рейтинг выбирается на основе следующих рекомендаций.

1) Высокое выравнивание (соответствие)

Для высокой согласованности предпосылок должна быть значительная часть целевой аудитории, для которой предпосылка соответствует рабочим обязанностям или практикам, в высшей степени правдоподобна и/или тесно связана с событием, имеющим отношение к аудитории. Например, если группа получателей — финансовый отдел, а фишинговое сообщение имеет предпосылку о просроченном или пропущенном платеже, общая согласованность высока.

2) Среднее выравнивание (соответствие)

Среднее соответствие достигается в любом случае: (i) когда предпосылка имеет правдоподобное, но слабое контекстное соответствие большой части целевой аудитории, или (ii) когда предпосылка имеет среднее контекстное соответствие небольшой части целевой аудитории. Например, если группа получателей в основном работает в одном физическом месте, а фишинговое сообщение имеет умеренно подходящую предпосылку для нескольких членов группы получателей, которые работают в другом физическом месте.

3) Низкое выравнивание (соответствие)

Существует низкое соответствие, когда предпосылка относится к теме, которая не имеет отношения к целевой аудитории или не правдоподобна. Например, если получателем является финансовый отдел, а предпосылка фишингового сообщения относится к конкурсу статей по биотехнологическим исследованиям или аналогичной несвязанной теме, общее соответствие будет низким.

**Метод 2: Формульный подход к категоризации выравнивания (соответствия) предпосылок**

В этом подходе используется набор из пяти элементов, каждый из которых оценивается по 5-балльной шкале. Общий балл, определенный из рейтингов, дает значение, отражающее категоризацию выравнивания предпосылок. Эти элементы были выбраны потому, что они представляют собой аспекты, связанные с согласованием предпосылок, которые организатор обучения может классифицировать для целевой группы обучающихся. Элементы предпосылки сообщения:

*Имитирует процесс или практику на рабочем месте:* этот элемент пытается отразить согласованность предпосылки с процессом или практикой на рабочем месте для целевой аудитории.

*Имеет отношение к рабочему месту:* этот элемент пытается отразить актуальность помещения для целевой аудитории,

*Согласуется с другими ситуациями или событиями*, в том числе внешними по отношению к рабочему месту: согласование с другими ситуациями или событиями, даже внешними по отношению к рабочему месту, придает сообщению ощущение знакомой проблемы.

*Вызывает беспокойство по поводу последствий отказа от нажатия*: потенциально опасные последствия отказа от нажатия повышают вероятность нажатия [3],

*Был предметом целевого обучения, специальных предупреждений или другого воздействия*: этот элемент предназначен для отражения целевых эффектов обучения, которые могут привести к обнаружению предпосылок. Необходимо позаботиться о том, чтобы должным образом включить специфику обучения или предупреждения, поскольку передача обучения довольно сложна [38].

Мы используем следующую 5-балльную рейтинговую шкалу с четными числовыми значениями от нуля до восьми с этими связанными якорями:

*8 = Чрезвычайная применимость, согласованность или релевантность*

*6 = Значительная применимость, согласованность или релевантность*

*4 = умеренная применимость, согласованность или релевантность*

*2 = Низкая применимость, согласованность или релевантность*

*0 = неприменимо, нет согласования или релевантности*

Общая оценка согласованности (соответствия) предпосылок конкретного фишинга и его целевой аудитории представляет собой сумму оценок элементов с 1 по 4. Поскольку пятый элемент относится к обучению предпосылке и помогает в обнаружении, его оценка вычитается из общей суммы. Наивысший возможный балл — 32, что указывает на очень высокую согласованность предпосылок. Наименьший возможный балл равен −8, что свидетельствует о крайне низком соответствии предпосылкам.

**Применение шкалы Фиша**

В этом разделе мы представляем данные десяти учебных упражнений по фишингу и используем шкалу фишинга для определения рейтинга сложности обнаружения для каждого упражнения. Данные упражнений, использованные здесь, получены из проекта, который был начат в 2012 году Отделом безопасности информационных технологий и сетей (ITSND) в NIST в качестве долгосрочного пробного развертывания встроенной программы повышения осведомленности. Пробное развертывание было рассчитано на несколько лет и использовало коммерчески доступную систему для помощи в разработке и доставке фишинговых сообщений и обучении, а также для отслеживания частоты кликов. Одна и та же система использовалась на протяжении всего 5+ летнего периода.

Для всех учений, кроме двух последних, проводившихся в рамках испытания, целевым населением в институте была одна операционная единица (OU), насчитывающая примерно 70 сотрудников. Обучение по повышению осведомленности, проводимое в рамках этих учений, дополняло обучение по вопросам безопасности ИТ, ежегодно проводимое всеми сотрудниками института. Сотрудники OU знали, что их подразделение участвует в судебном процессе. Эти учения проводились сотрудником по безопасности информационных технологий (ITSO) OU. Один и тот же человек занимал эту должность в течение всего испытательного срока. ITSO выбрало фишинговое сообщение и его предпосылку из шаблонов, предоставленных системой обучения, которые имитировали текущие реальные угрозы. Некоторые сообщения были адаптированы для соответствия деловым и коммуникационным практикам внутри организации или были персонализированы, другими словами, они были фишинговыми [39]. Целевой аудиторией для двух оставшихся учений был весь персонал NIST. Во всех упражнениях обучающие электронные письма по фишингу моделировали фишинговые кампании в реальном мире, а участвующие сотрудники находились в своей обычной рабочей среде с их регулярной рабочей нагрузкой, что обеспечивало экологическую достоверность. Все учения были необъявленными и проводились через нерегулярные промежутки времени, чтобы избежать предварительных эффектов. Данные были собраны с соответствующего одобрения испытуемых в Национальном институте стандартов и технологий (NIST).

Во-первых, мы даем описание каждого упражнения, его обоснование согласования предпосылок (метод 1), рейтинги элементов согласования предпосылок и общий балл (метод 2), а также краткое описание целевой аудитории и ее размера. Затем мы собираем данные в Таблицу 13 , включая наблюдаемые подсчеты сигналов, представленные в

Дополнительное приложение A показывает рейтинг сложности обнаружения для каждого упражнения рядом с фактической частотой кликов.

**Таблица 8:**

упражнение на день святого валентина, выравнивание предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг Мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 0 (не применимо) |
| Имеет отношение к рабочему месту | 2 (низкий) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 6 (значительный) |
| Вызывает беспокойство о последствиях отказа от клика | 2 (низкий) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий | 10 |

Каждому упражнению присвоена метка, относящаяся к сценарию, например, требования безопасности, а также номер упражнения, E1, E2, … и т. д., относящийся к порядку представления, который упорядочен по частоте кликов. Обратите внимание, что, хотя мы присвоили этим упражнениям рейтинги по категориям соответствия предпосылкам, а не проводникам обучения самостоятельно, мы сделали это при соответствующем вкладе исполнителей обучения. Изображение каждого фишингового сообщения представлено в Дополнительном приложении B. Эти изображения воссоздают реальные снимки экрана сообщений, хотя получатели сообщений были заменены вымышленными именами.

Упражнения E3, E5 и E7 — новая голосовая почта, неоплаченный счет и подтверждение заказа, соответственно, первоначально были описаны в Greene et al. [3]. Упражнения E1, E2, E6 и E8 — требования безопасности (ранее называвшиеся «Gmail»), блоги, Valentine и токен безопасности соответственно были первоначально представлены в исх. [18. Упражнения E4, E9 и E10 — «Отсканированный файл», «Подарочный сертификат» и «Обновление Adobe» соответственно представляют новые данные.

**Описание упражнений по фишингу**

Требования безопасности 2 (Е1)

Описание сообщения: Фишинг требований безопасности был особенно хитрым целевым фишингом. Он нацеливался на сотрудников, использующих поддельный адрес Gmail высшего руководства, тактика, основанная на реальном фишинге, ранее наблюдаемом в NIST. Оказалось, что фишинг в реальном мире исходил из личной учетной записи Gmail директора NIST (firstname.lastname1@gmail.com) и попадал в список руководителей лаборатории. Фишинг с учебными упражнениями также, по-видимому, исходил от высшего руководства NIST, директора организационного подразделения (OU), и выглядел как (firstname.lastname1@gmail.com). Сходства сохранялись в строке темы, теле и заключительных частях электронного письма. Тема сообщения была «ПОЖАЛУЙСТА, ПРОЧИТАЙТЕ ЭТО», что важно, учитывая, что NIST уделяет очень большое внимание развитию культуры безопасности. Электронное письмо было персонализировано с указанием имени получателя. Тело сказало: «Я настоятельно рекомендую вам прочитать это». В следующей строке была ссылка со следующим текстом, выделенным жирным шрифтом, «Требования безопасности». Электронное письмо было подписано просто словами «С уважением» и именем директора OU.

Согласование предпосылок (Метод 1): соответствие классифицируется как высокое — согласование предпосылок очень сильное, учитывая значительный акцент более крупной организации на безопасности на рабочем месте и то, что сообщение, по-видимому, исходило от высшего руководства NIST, известного как авторитетная фигура в этом контексте. Согласованность еще больше усиливается ответственностью целевого отдела за охрану труда и технику безопасности в более крупной организации.

Согласование предпосылок (Метод 2): Общее соответствие составляет 30 из 32 возможных. В таблице 3 показана присвоенная оценка для каждого элемента в формульном методе и сумма.

**Таблица 3:**

Упражнение по требованиям безопасности, выравнивание помещения, оценка метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 8 (Экстремальный) |
| Имеет отношение к рабочему месту | 8 (Экстремальный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 8 (Экстремальный) |
| Вызывает беспокойство о последствиях отказа от клика | 8 (Экстремальный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | −2 (низкий) |
| Общее выравнивание | 30 |

Целевая аудитория: одно подразделение в NIST, занимающееся финансовыми вопросами (заказы и выверка счетов), административная поддержка программ и техническая поддержка программ, n  =  73.

**Блоги (E2)**

Описание сообщения: Фишинг в блогах был еще одним целевым фишингом. Оказалось, что оно пришло от системного администратора с адресом электронной почты, note@nist.gov . Тема письма была «Несанкционированный доступ к веб-сайту». Персонализации не было. Орган заявил: \*Это автоматическое электронное письмо\*. Наши регулирующие органы требуют, чтобы мы отслеживали и ограничивали доступ к определенным веб-сайтам из-за содержания. Система фильтров пометила ваш компьютер как тот, который просматривал веб-сайты с ограниченным контентом или заходил на них. Система не является надежной и может неправильно помечать ограниченное содержимое. ИТ-отдел не расследует каждое сообщение веб-фильтра, но может принять дисциплинарные меры». Жирным шрифтом было сказано: «Немедленно войдите в систему фильтрации со своими сетевыми учетными данными и просмотрите свои журналы, чтобы увидеть, какие веб-сайты вызвали это предупреждение». Далее следовала ссылка с пометкой «Журналы веб-безопасности». Контактная информация не была указана, а электронное письмо закрывалось словами: «Не отвечайте на это письмо. Это электронное письмо было создано автоматически, чтобы сообщить вам о нарушении нашей политики безопасности и содержания».

*Соответствие предпосылке (Метод 1):* Соответствие оценивается как высокое — предпосылка согласуется с тем фактом, что доступ к неприемлемому контенту действительно является нарушением политики правил поведения организации и может быть основанием для увольнения любого сотрудника организации. Предпосылка основывается на том факте, что многие организации, в том числе NIST, регулярно сканируют данные журналов. Компонент угрозы в сочетании с тяжестью последствий увеличивает расклад. Следует отметить, что все новые сотрудники проходят очное обучение правилам поведения и политике организации в области информационных технологий (ИТ), где особое внимание уделяется дисциплинарным взысканиям, связанным с ненадлежащим просмотром веб-контента.

*Выравнивание предпосылок (Метод 2):* Общее соответствие составляет 16 из 32 возможных. В таблице 9 показаны присвоенный рейтинг для каждого элемента в формульном методе и сумма.

**Таблица 4:**

упражнение в блогах, выравнивание предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 8 (Экстремальный) |
| Имеет отношение к рабочему месту | 8 (Экстремальный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 0 (не применимо) |
| Вызывает беспокойство о последствиях отказа от клика | 8 (Экстремальный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий | 24 |

Целевая аудитория: одно подразделение в NIST, занимающееся финансовыми вопросами (заказы и выверка счетов), административная поддержка программ и техническая поддержка программ, n  =  64.

**Неоплаченный счет (E3)**

Описание сообщения: фишинговый неоплаченный счет был отправлен вымышленным сотрудником того же учреждения, что и получатель электронной почты, коллегой по имени Джилл Престон ( jill.preston@nist.gov ). Тема письма: «Неоплаченный счет № 4806». Приветствие было персонализировано словами «Уважаемый [Имя Фамилия]». В теле письма говорилось: «Пожалуйста, ознакомьтесь с прикрепленным счетом (.doc) и переведите платеж в соответствии с условиями, указанными в нижней части счета. Дайте нам знать, если у вас есть какие-либо вопросы. Мы высоко ценим ваше оперативное внимание к этому вопросу!» Электронное письмо просто закрывалось именем «Джилл Престон». Никакой другой контактной информации под именем не было. Следует отметить, что имело место несоответствие расширения файла между тем, как вложение упоминалось в теле письма (как .doc ) и то, как было помечено само вложение, оказалось, что это .zip с именем файла «invoice\_S-37644806.zip». Фишинг с неоплаченными счетами имитировал программу-вымогатель Locky [ 39 ], реальную угрозу того времени.

*Согласование предпосылок (Метод 1):* соответствие классифицируется как высокое — предпосылки чрезвычайно высоко согласованы примерно для трети целевой аудитории и несколько согласованы для остального отдела. Кроме того, все целевое подразделение было предупреждено о любых неоплаченных счетах после недавнего события, связанного с законным неоплаченным счетом.

*Согласование предпосылок (метод 2):* общее соответствие составляет 24 из 32 возможных. В таблице 5 показаны присвоенные рейтинги для каждого элемента в формульном методе и сумма.

**Таблица 5:**

неоплаченный счет-фактура, выравнивание помещения, рейтинги метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 4 (умеренный) |
| Имеет отношение к рабочему месту | 8 (Экстремальный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 6 (значительный) |
| Вызывает беспокойство о последствиях отказа от клика | 6 (значительный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий | 24 |

Целевая аудитория: одно подразделение в NIST, занимающееся финансовыми вопросами (заказы и выверка счетов), административная поддержка программ и техническая поддержка программ. п  =  73

**Отсканированный файл (E4)**

Описание сообщения: фишинговый отсканированный файл поступил от «LaserPro\_2\_2\_e» с адресом электронной почты «laerpro\_2\_2\_e @nagts.org». Тема письма была «Сканирование с Laser Pro i780 Second Floor». Персонализации не было. Тело содержало текст: «Пожалуйста, откройте вложение. Он был отсканирован и отправлен на Laser Pro i789». За этим текстом следовали «SENT BY: INELL», «PAGES: 1» и «FILETYPE: .DOC», каждая в последовательных строках. В нижней части письма было изображение, указывающее на вложенный файл и имя файла «SCN001375.doc», завершающее фишинг.

Предпосылка выравнивания (метод 1): выравнивание относится к категории высокого уровня — сообщение основано на общепринятой деловой практике с использованием общего устройства сканирования и печати. Кроме того, в подразделении недавно было установлено новое большое совместно используемое принтерное устройство. Кроме того, приложенный документ якобы был отсканирован внутри компании и, вероятно, казался заслуживающим доверия, в то же время, вызывая любопытство к содержимому и, возможно, к возможности передачи отсканированного файла предполагаемому получателю.

Согласование предпосылок (Метод 2): Общее соответствие составляет 18 из 32 возможных. В таблице 6 показаны присвоенный рейтинг для каждого элемента в формульном методе и сумма.

**Таблица 6:**

упражнение с отсканированным файлом, выравнивание предпосылок, оценки метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 6 (значительный) |
| Имеет отношение к рабочему месту | 4 (умеренный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 6 (значительный) |
| Вызывает беспокойство о последствиях отказа от клика | 4 (умеренный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | −2 (низкий) |
| Общий | 18 |

**Новая голосовая почта (E5)**

*Описание сообщения*: Новый фишинг голосовой почты оказался от вымышленной корпоративной виртуальной машины (corpvm@webaccess-alert.com). Похоже, это было сгенерированное системой электронное письмо с темой, которая гласила: «У вас новая голосовая почта». В верхней части письма был большой черно-зеленый баннер с белым текстом «CorpVM». В электронном письме не было логотипов, однако был небольшой черный нижний колонтитул с надписью «© 2015 CorpVM Inc.». в белом. Текст письма начинался словами «У вас новая голосовая почта!» текст выделен жирным шрифтом по центру, за которым следует «От: неизвестный абонент, получено: 06.03.2016, продолжительность: 00:52». Под этим текстом была персонализированная строка [Имя Фамилия], за которой следовала фраза: «Вы получили это сообщение, потому что мы не смогли его доставить. Голосовое сообщение не прошло, потому что в тот момент голосовая почта была недоступна. Чтобы прослушать это сообщение, нажмите здесь . У вас должны быть включены динамики, чтобы прослушать сообщение. \* Номер ссылки для этого сообщения: qvfl\_cjl09-9107319601-2125579909-62. Продолжительность передачи составила примерно 52 секунды. Идентификатор принимающей машины: YJH35-TW410-F37JZL. Спасибо." Наконец, электронное письмо закрывалось более мелким текстом, выделенным курсивом, который гласил: «Это системное сообщение с адреса только для отправки. Пожалуйста, не отвечайте на это письмо"

*Согласование предпосылок* (метод 1): согласование классифицируется как среднее — предпосылка была правдоподобной. Примерно в то же время, что и учения, внедрялся новый бизнес-процесс для уведомления голосовой почты, а не доставки, хотя и без особой помпы. Несмотря на то, что предпосылка была правдоподобной, она отсутствовала или была слабо связана с контекстом для большей части, хотя и не для всех, целевой аудитории на основе отзывов об опросе, представленных в исх. [ 3 ].

*Согласование предпосылок (Метод 2*): Общее соответствие составляет 16 из 32 возможных баллов. В таблице 7 показан присвоенный рейтинг для каждого элемента в формульном методе и сумма.

**Таблица 7:**

новое упражнение голосовой почты, согласование предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 6 (значительный) |
| Имеет отношение к рабочему месту | 4 (умеренный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 2 (низкий) |
| Вызывает беспокойство о последствиях отказа от клика | 4 (умеренный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | −2 (низкий) |
| Общий |  |

Целевая аудитория: одно операционное подразделение (OU) в NIST, занимающееся финансовыми вопросами (заказы и выверка счетов), административная поддержка программ и техническая поддержка программ, n  =  69.

**Валентин (E6)**

Описание сообщения: фишинг на День святого Валентина, по-видимому, пришел из «Доставки электронных открыток» с адресом электронной почты «do\_not\_reply@ecardalert.com». В теме письма говорилось: «С Днем святого Валентина! Посмотрите, кто прислал вам электронную открытку…» В верхней части письма было три больших красных сердечка. Персонализации не было. В теле письма говорилось: «Тайный поклонник поздравил тебя с Днем святого Валентина! Некоторые из вас, возможно, слышали о наших поздравительных открытках для сотрудников, которые можно использовать для поздравления коллег. Нажмите на ссылку ниже, чтобы просмотреть свою». Далее следовала большая ссылка «Ваша карта ожидает» и дополнительный текст: «Если у вас возникли проблемы с просмотром электронной карты, нажмите здесь». «Вы хотите отправить электронную открытку? Посетите наш сайт. Делая чей-то день, по одной электронной открытке за раз…» Электронное письмо заканчивалось словами: «Это электронное письмо может содержать конфиденциальную и привилегированную информацию для исключительного использования предполагаемым получателем. Если вы не являетесь предполагаемым получателем, свяжитесь с отправителем и удалите все копии. Любое рассмотрение или распространение другими лицами строго запрещено. Спасибо." Фиш-валентинка была отправлена ​​22 января 2018 года, накануне Дня святого Валентина.

*Согласование предпосылок (Метод 1):* согласование относится к категории низкого уровня — основная предпосылка, связанная с Днем святого Валентина, не согласуется с бизнес-процессом, а носит более личный характер. Однако в сообщении упоминается признание коллеги по работе, что рекомендуется на рабочем месте. Таким образом, хотя основная предпосылка не соответствует деловой практике, она играет на любопытстве читателя, согласуясь с предстоящим Днем святого Валентина, о котором знает большинство людей.

*Согласование предпосылок (Метод 2):* Общее соответствие составляет 10 из 32 возможных баллов. В таблице 8 показаны присвоенные рейтинги для каждого элемента в формульном методе и сумма.

Целевая аудитория: все сотрудники NIST, имеющие адрес электронной почты, были нацелены на всех сотрудников NIST, от отдела кадров до финансового отдела, научных сотрудников, административной поддержки и всех уровней управления, n  =  4 977.

**Подтверждение заказа (E7)**

Описание сообщения: Фишинг с подтверждением заказа, по-видимому, был отправлен из «Подтверждения заказа» (auto-confirm@discontcomputers.com). Обратите внимание на неправильное написание слова «скидка» в адресе электронной почты. Строка темы была персонализирована и гласила: «[Имя Фамилия]Ваш заказ обработан» без пробела между фамилией пользователя и словом «Ваш». В верхней части письма было изображение нескольких праздничных пакетов со словами «Подтверждение заказа», выделенными жирным шрифтом сразу под изображением праздничного пакета. В теле письма не было ни персонализации, ни какого-либо приветствия. В основном тексте электронного письма говорилось: «Спасибо, что сделали заказ у нас. Ваш заказ был обработан. Когда ваш товар будет отправлен, мы отправим электронное письмо с подтверждением». Затем следовали слова «Детали заказа» оранжевым цветом и «Заказ: #SGH-2548883-2619437» (номер заказа был выделен синим цветом). В следующем разделе письма говорилось: «Предполагаемая дата доставки: 02.12.2016» (дата была выделена зеленым текстом). «Промежуточная сумма: 59,97 долларов США», «Расчетный налог: 4,05 доллара США» и «Общая сумма заказа: 64,02 доллара США» выделены жирным шрифтом. Там была большая желтая кнопка с надписью «Управление заказом». За кнопкой следовал текст: «Спасибо за заказ. Мы надеемся, что вы скоро вернетесь за новыми удивительными предложениями». Внизу письма было изображение праздничного снежного шара и текст: «Нужен к праздникам? Закажите до 23 декабря и получите бесплатную доставку в ночное время». («23 декабря» было выделено синим цветом). Гораздо меньший серый текст ниже гласил: «Если не указано иное, проданные товары облагаются налогом с продаж в соответствии с местным законодательством. Для получения дополнительной информации, пожалуйста, просмотрите налоговую информацию» («налоговая информация» была выделена синим цветом). Обратите внимание на повторяющееся слово «in in», тонкую ошибку, которую пользователям очень трудно заметить, особенно с учетом мелкого серого шрифта. Окончательно, в самом низу письма появились три дополнительные ссылки, все синим цветом в одной строке: «Политика возврата | Конфиденциальность | Счет."

*Согласование предпосылок (Метод 1):* согласование относится к категории Среднее — соответствие предпосылок для тех, у кого были полномочия на закупку в ОП, и для тех, кто недавно разместил заказ, небольшой подмножество всей ОП. Тем не менее, учения проходили в декабре, когда многие люди делают онлайн-покупки к праздникам.

Согласование предпосылок (метод 2): общее соответствие составляет 16 из 32 возможных. В таблице 9 показаны присвоенные рейтинги для каждого элемента в формульном методе и сумма.

**Таблица 9:**

упражнение по подтверждению заказа, выравнивание предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 4 (умеренный) |
| Имеет отношение к рабочему месту | 2 (низкий) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 6 (значительный) |
| Вызывает беспокойство о последствиях отказа от клика | 4 (умеренный) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий | 16 |

Маркер безопасности (E8)

Описание сообщения: Фишинг с токеном безопасности оказался из «Оповещений» с адресом электронной почты « alerts@verifytoken.com ». Строка темы была «Убедитесь, что ваш токен безопасности не был скомпрометирован». Электронное письмо было персонализировано с использованием формата «Фамилия, Имя, Отчество (Fed)». Орган сказал: «Недавно нам стало известно о нарушении безопасности в нашем продукте токена безопасности. Некоторые токены были скомпрометированы и, возможно, их необходимо заменить. Чтобы узнать, был ли скомпрометирован ваш токен [sic], проверьте свой токен безопасности здесь.». (Обратите внимание на «ваш токен» вместо «ваш токен».) Электронное письмо было подписано «Ривест Шамир Адлеман, директор по управлению идентификацией и доступом». Электронное письмо закрывалось текстом меньшего размера, в котором говорилось: «Это электронное письмо может содержать конфиденциальную и привилегированную информацию для исключительного использования предполагаемым получателем. Любое рассмотрение или распространение другими лицами строго запрещено. Если вы не являетесь предполагаемым получателем, свяжитесь с отправителем и удалите все копии. Спасибо." Если кто-то щелкнул ссылку «Подтвердите свой токен безопасности здесь», он попадал на веб-страницу ввода данных с URL-адресом «secure.verifytoken.com». В верхней части веб-страницы было написано «Token Security» на красном фоне, а затем «Внимание!!! Недавно безопасность некоторых токенов безопасности была скомпрометирована. Введите свое имя пользователя и шестизначное число, которое генерируется каждые 60 секунд вашим токеном безопасности, и мы узнаем, понадобится ли вам новый токен. Если вам понадобится новый токен, вам будет предоставлена ​​контактная информация для запроса нового токена, который будет отправлен вам в одночасье». Затем следовал текст «Вход в учетную запись» с полями, помеченными как «Идентификатор пользователя» и «Пароль или пароль». Там была синяя кнопка с надписью «Войти» и флажок «Я не робот». Внизу веб-страницы был текст: «Код доступа содержит PIN-код и число из токена безопасности». Там была синяя кнопка с надписью «Войти» и флажок «Я не робот». Внизу веб-страницы был текст: «Код доступа содержит PIN-код и число из токена безопасности». Там была синяя кнопка с надписью «Войти» и флажок «Я не робот». Внизу веб-страницы был текст: «Код доступа содержит PIN-код и число из токена безопасности».

Выравнивание предпосылок (метод 1): выравнивание относится к категории средних — предпосылка вообще не выравнивается для тех сотрудников, у которых нет токена безопасности (примерно 43% всех сотрудников в организации). Кроме того, предпосылка не согласуется с теми сотрудниками, которые ожидают, что любая проверка и замена токенов будет проводиться через организацию, а не через третью сторону — вероятно, значительная часть оставшихся 57%, поскольку организация занимает очень сильную позицию в отношении ИТ-безопасности.

Согласование предпосылок (метод 2): общее соответствие составляет 12 из 32 возможных. В таблице 10 показаны присвоенные рейтинги для каждого элемента в формульном методе и сумма.

**Таблица 10:**

упражнение с жетоном безопасности, согласование предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 2 (низкий) |
| Имеет отношение к рабочему месту | 6 (значительный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 2 (низкий) |
| Вызывает беспокойство о последствиях отказа от клика | 2 (низкий) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий |  |

Подарочный сертификат (Е9)

Описание сообщения:Поддельный подарочный сертификат оказался от «HR Rewards» с адресом электронной почты «certificates@great-restaurant-deals.com». Тема письма была «Ваш подарочный сертификат ресторана здесь!» Основная часть письма содержала изображение в зеленом, коричнево-сером и сером цветах, показывающее людей в ресторане; графическое изображение было озаглавлено «Ваш подарочный сертификат ресторана прилагается!» Электронное письмо было персонализировано с использованием формата «Привет [Имя Фамилия]!» После приветствия электронное письмо гласило: «Ваш БЕСПЛАТНЫЙ дополнительный подарочный сертификат ресторана прибыл!» Обратите внимание на неправильное использование слова «дополнительный», а не «дополнительный». Слева от сообщения был текст: «Просто скачайте и распечатайте прикрепленный купон и используйте его в любом месте или по вашему выбору! (Пожалуйста, убедитесь, что штрих-код вложения печатается четко. )» Справа от этого текста был большой коричневый прямоугольник с текстом «Экономия 25%!» Ниже было восклицание: «Счастливого ужина!» Другой прямоугольник зеленого цвета содержал текст: «Пожалуйста, ознакомьтесь с дополнительными сведениями и ограничениями в нижней части официального купона, который прилагается. Срок действия предложения истекает через 14 дней с даты получения этого письма». Сообщение заканчивалось текстом «© 2014, все права защищены».

Соответствие предпосылке (Метод 1): Соответствие классифицируется как низкое — отдел кадров NIST не выдает подарочные сертификаты. Предпосылка основана на потенциальном желании читателя получить подарочный сертификат на 25% в ресторан по своему выбору.

Выравнивание по предпосылкам (метод 2): общее соответствие составляет 2 из 32 возможных. В таблице 11 показана присвоенная оценка для каждого элемента в формульном методе и сумма.

**Таблица 11:**

упражнение с подарочным сертификатом, выравнивание предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 0 (не применимо) |
| Имеет отношение к рабочему месту | 0 (не применимо) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 0 (не применимо) |
| Вызывает беспокойство о последствиях отказа от клика | 2 (низкий) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | 0 (не применимо) |
| Общий | 2 |

Обновление Adobe (E10)

Описание сообщения: фишинговое обновление Adobe оказалось отправленным из «Adobe Alerts» с адресом электронной почты « adobeupdates@applerts.net ».». Строка темы была «Последнее обновление безопасности Adobe». Электронное письмо имело «высокий» уровень важности в информации заголовка. Электронное письмо не было персонализировано, и в нем не было приветствия. Первые две строки тела письма содержали «Бюллетень по безопасности» и «Обновления безопасности, доступные для Adobe Reader и Acrobat». «Дата выпуска» «12 февраля 2015 г.» была указана за пять дней до даты отправки электронного письма. Следующая строка текста содержала следующее: «Идентификаторы уязвимостей: APSB11-24». Затем последовали «номера CVE: CVE-2011-1353, CVE-2011-2431, CVE-2011-2432, CVE-2011-2433, CVE-2011-2434, CVE-2011-2435, CVE-2011-2436, CVE-2011-2437, CVE-2011-2438, CVE-2011-2439, CVE-2011-2440, CVE-2011-2441, CVE-2011-2442». За номерами CVE следовала фраза «Платформа: все». Далее было одно слово «РЕЗЮМЕ» и следующий текст: «Критические уязвимости были обнаружены в Adobe Reader XI (11.0.04) и более ранних версиях для Windows и Macintosh, Adobe Reader 9.5.5 и более ранних версиях для UNIX, а также Adobe Acrobat XI и более ранних версиях для Windows и Macintosh. Эти уязвимости могут привести к сбою приложения и потенциально позволить злоумышленнику получить контроль над уязвимой системой». За «резюме» следовал текст: «Нажмите здесь , чтобы загрузить и установить обновление». Последняя строка письма содержала текст: «Более подробную информацию и информацию о решении можно найти здесь ». Ни закрытия, ни контактной информации не было.

Соответствие предпосылкам (Метод 1): Соответствие классифицируется как низкое — предпосылка согласуется с тем фактом, что почти у всех сотрудников на компьютерах были Adobe Reader или Acrobat; однако процесс обновления, инициированный по электронной почте, совершенно не соответствовал общепринятому NIST процессу обновления программного обеспечения.

Согласование предпосылок (Метод 2): Общее соответствие составляет 4 из 32 возможных. В таблице 12 показаны присвоенный рейтинг для каждого элемента в формульном методе и сумма.

**Таблица 12:**

Упражнение по обновлению Adobe, выравнивание предпосылок, рейтинг метода 2

| **Элемент выравнивания помещения** | **Рейтинг мировоззрения** |
| --- | --- |
| Имитирует рабочий процесс или практику | 0 (не применимо) |
| Имеет отношение к рабочему месту | 4 (умеренный) |
| Согласуется с другими ситуациями или событиями, в том числе внешними по отношению к рабочему месту | 0 (не применимо) |
| Вызывает беспокойство о последствиях отказа от клика | 2 (низкий) |
| Был предметом целенаправленного обучения, конкретных предупреждений или другого воздействия | −2 (низкий) |
| Общий | 4 |

Определение оценок сложности

Применение шкалы Фиша

Как описано ранее, рейтинг сложности для отдельного фишингового сообщения определяется сначала путем категоризации количества объективно наблюдаемых сигналов и выравнивания предпосылок. Эта пара категорий используется для выбора оценки сложности обнаружения по шкале фишинга, показанной в концептуальной структуре в таблице 1 , для фишингового сообщения для определенной целевой аудитории. В таблице 13 показаны рейтинги по шкале фишинга для каждого из десяти способов фишинга, описанных в последнем разделе, включая количество признаков для каждого электронного письма (подробности приведены вДополнительное приложение A), согласование предпосылок — Методы 1 и 2 — (из описания упражнения и обсуждения с организатором обучения), рейтинг сложности (из концептуальной основы в Таблице 1 ) и фактическое количество кликов по каждому упражнению.

**Таблица 13:**

данные об упражнениях по фишингу

| **Номер упражнения** | **Название упражнения** | **Тип атаки** | **Количество сигналов** | **Выравнивание помещения (метод 1)** | **Выравнивание помещений (метод 2)** | **Рейтинг сложности** | **Фактическая частота фишинговых кликов** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Е1 | Требования безопасности ( *n* = 73) | Ссылка на сайт | 7 (Несколько) | Высокая | 30 (высокий) | Очень сложно | 49,3% (36/73) |
| Е2 | Веблоги ( *n* = 64) | Ссылка на сайт | 14 (Некоторые) | Высокая | 24 (высокий) | Очень сложно | 43,8% (28/64) |
| Е3 | Неоплаченный счет ( *n* = 73) | Вложение | 8 (Несколько) | Высокая | 24 (высокий) | Очень сложно | 20,5% (15/73) |
| Е4 | Отсканированный файл ( *n* = 62) | Вложение | 6 (Несколько) | Высокая | 18 (высокий) | Очень сложно | 19,4% (12/62) |
| Е5 | Новая голосовая почта ( *n* = 69) | Ссылка на сайт | 11 (Некоторые) | Середина | 14 (средний) | Умеренно сложный | 11,6% (8/69) |
| Е6 | Валентина ( *n* = 4 097) | Ссылка на сайт | 13 (Некоторые) | Низкий | 10 (низкий) | Умеренно/Наименее сложно | 11,0% (549/4 977) |
| Е7 | Подтверждение заказа ( *n* = 66) | Ссылка на сайт | 18 (много) | Середина | 16 (средний) | Умеренно сложный | 9,1% (6/66) |
| Е8 | Токен безопасности ( *n* = 5 024) | Сбор учетных данных по ссылке | 12 (Некоторые) | Середина | 12 (средний) | Умеренно сложный | 8,7% (439/5 024) |
| Е9 | Подарочный сертификат ( *n* = 63) | Вложение | 11 (Некоторые) | Низкий | 2 (низкий) | Умеренно/Наименее сложно | 4,8% (3/63) |
| Е10 | Обновление Adobe ( *n* = 63) | Ссылка на сайт | 12 (Некоторые) | Низкий | 4 (низкий) | Умеренно/Наименее сложно | 3,2% (2/63) |

Таблица вДополнительное Приложение А содержит количество для каждой реплики и общее количество для каждого упражнения. При подсчете реплик в данном сообщении электронной почты во время анализа важно отметить, что эти подсчеты основаны на нашем чрезвычайно тщательном изучении сообщений электронной почты; большинство пользователей электронной почты не заметят и не прислушаются ко всем доступным сигналам.

Обратите внимание, что для расчета рейтинга сложности количество сигналов должно быть дополнительно разделено на несколько , несколько или много в порядке убывания сложности. Хотя некоторые сигналы более заметны, чем другие, мы ожидаем, что это разумное первое приближение. В этой первоначальной версии шкалы Фиша мы предлагаем связанные диапазоны следующим образом: категория с надписью « Мало» представлена ​​1–8 признаками, категория с обозначением « Некоторые » — 9–14 признаками, а категория с обозначением « Много » — 15 или более признаками.

Кроме того, мы предлагаем, чтобы оценки выравнивания предпосылок были связаны со следующими оценками с использованием Метода 2: Высокое выравнивание достигается при общем балле 18 и выше, Среднее выравнивание достигается при общем балле от 10 до 18, а Низкое выравнивание достигается при общем балле от 10 до 18. общий балл 10 и ниже.

Эти диапазоны основаны на нашем существующем наборе данных; на этом этапе разработки шкалы количество кликов дает информацию для категоризации количества реплик и оценок выравнивания предпосылок. Мы полностью ожидаем, что эти диапазоны могут измениться с более широким применением шкалы фишинга к большему количеству фишинговых писем. Чтобы сначала сообщить диапазоны, требуется больший корпус фишинговых писем, а затем требуется дополнительный корпус фишинговых писем для проверки диапазонов.

Следует подчеркнуть, что количество сигналов или выравнивание предпосылок сами по себе не определяют сложность обнаружения для целевой аудитории; это только тогда, когда эти элементы рассматриваются вместе для целевой аудитории , можно вычислить рейтинг сложности обнаружения.

Фишинг с токеном безопасности был единственным упражнением с компонентом ввода данных — после перехода по ссылке пользователи попадали на веб-страницу, запрашивающую их учетные данные. Мы приводим показатели ввода данных здесь, а не в Таблице 13 . Для фишинга с токенами безопасности 24,4% (107/439) кликеров вводили данные на веб-странице сбора учетных данных. Однако это всего 2,1% (107/5024) от общего числа сотрудников, получивших фишинговое письмо. Учитывая, что примерно 75% кликеров не вводили данные на веб-странице, кажется, что на этой странице были вызваны дополнительные подозрения, вероятно, из-за запроса учетных данных. Это, безусловно, согласуется с тем фактом, что обязательные ежегодные тренинги по безопасности в NIST в прошлом были в значительной степени сосредоточены на том, чтобы не делиться учетными данными.

Наблюдения

С помощью этих десяти фишинговых упражнений мы применили нашу шкалу фишинга к различным типам фишинговых атак. Сюда входят атаки на основе ссылок (требования безопасности, блоги, новая голосовая почта, Валентина, подтверждение заказа и обновление Adobe), атаки на вложения (неоплаченный счет, имитирующий реальную атаку программы-вымогателя Locky, отсканированный файл и подарочный сертификат) и атака ввода данных или сбора учетных данных (токен безопасности). Теперь, когда мы использовали шкалу фишинга для определения рейтинга сложности обнаружения для десяти упражнений по фишингу, мы можем сделать несколько наблюдений.

Все упражнения с рейтингом сложности обнаружения « Очень сложно» также имеют относительно высокие показатели кликов (требования безопасности: 49,3%, блоги: 43,8%, неоплаченный счет: 20,5% и отсканированный файл: 19,4%). Тем не менее, в упражнении Weblogs гораздо больше сигналов, чем в трех других упражнениях, и при 14 сигналах он находится на крайнем конце диапазона некоторых сигналов (от 9 до 14).

Все упражнения с рейтингом сложности обнаружения « Умеренно сложно» имеют относительно более низкие показатели кликов (Новая голосовая почта: 11,6%, Подтверждение заказа: 9,1% и Токен безопасности: 8,7%). Точно так же упражнения, имеющие диапазон сложности обнаружения от умеренно сложного до наименее сложного (валентинка: 11,0%, подарочный сертификат: 4,7% и обновление Adobe 3,2%), имеют средний или низкий рейтинг кликов. Упражнения с жетонами Valentine и Security имеют относительно большую и разнообразную выборку, чем другие упражнения, что, вероятно, затрудняет классификацию соответствия предпосылок. И, наконец, у нас нет упражнения с рейтингом сложности обнаружения « Наименее сложно»., обращая внимание на необходимость применения шкалы Фиша к дополнительным упражнениям. В Таблице 14 мы возвращаемся к концептуальной структуре, приведенной в Таблице 1 , и отмечаем, какие категории представлены с представленными здесь операционными данными.

**Таблица 14:**

шкала Phish — охват категорий

| **Количество сигналов** | **Выравнивание помещения** | **Сложность обнаружения** | **Упражнение с кликабельностью** |
| --- | --- | --- | --- |
| Несколько (сложнее) | Высокая | Очень сложно | Требования безопасности (49,3%), |
| Неоплаченный счет (20,5%), |
| Отсканированный файл (19,4%) |
| Середина | Очень сложно | – |
| Низкий | Умеренно сложный | – |
| Немного | Высокая | Очень сложно | Веблоги (43,8%) |
| Середина | Умеренно сложный | Новая голосовая почта (11,6%) |
| Токен безопасности (8,7%) |
| Низкий | Умеренно или наименее сложно | Валентина (11,0 %) |
| Подарочный сертификат (4,8%) |
| Обновление Adobe (3,2%) |
| Много (менее сложно) | Высокая | Умеренно сложный | – |
| Середина | Умеренно сложный | Подтверждение заказа (9,1%) |
| Низкий | Наименее сложный | – |

Ограничения

Эта работа является ранней попыткой охарактеризовать сложность обнаружения фишинговых сообщений для пользователей электронной почты, находящихся в своей обычной среде обработки электронной почты. Таким образом, мы признаем, что в настоящее время у этой работы, безусловно, есть ограничения.

Текущие заметные ограничения в этой работе включают: (i) список сигналов длинный, но не исчерпывающий; (ii) неравномерная значимость реплик не учитывается при подсчете реплик, но может косвенно отражаться в выравнивании предпосылок; (iii) требуется больше опыта в категоризации соответствия предпосылок для улучшения руководства по оценке; (iv) диапазоны подсчета сигналов и диапазоны выравнивания предпосылок (метод 2) должны быть подтверждены дополнительными данными; и (v) необходимы дополнительные данные для проверки масштаба. Кроме того, дополнительные данные, используемые для информирования компонентов ареала и, в конечном счете, для проверки шкалы, должны поступать из различных групп населения и секторов.

Мы ожидаем, что каждое из этих ограничений будет устранено по мере дальнейшего развития шкалы Phish.

Обсуждение и будущие направления

Одних кликов недостаточно: почему важна сложность обнаружения фишинга

Директора по информационной безопасности, ответственные за надзор за встроенным обучением по вопросам фишинга, часто обеспокоены, когда они наблюдают, что количество кликов выше, чем ожидалось. Им остается недоумевать, почему рейтинг кликов продолжает меняться — возможно, включая большие всплески — несмотря на то, что они тратят значительные суммы денег и времени на обучение персонала. Директора по информационной безопасности должны обосновать свои бюджеты на обучение кибербезопасности и показать хорошую рентабельность инвестиций, чтобы их финансирование такого обучения не сократилось. К сожалению, если показатели кликов продолжают оставаться высокими или непостоянными, это часто — и мы утверждаем, что это неправильно — воспринимается как результат неэффективного обучения. Мы утверждаем, что это восприятие в корне неверно, и надеемся начать рассеивать его, разработав Шкалу Фиша. Кроме того, мы выступаем против сосредоточения внимания исключительно на количестве кликов по фишинговым упражнениям, и вместо этого настоятельно поощрять включение показателей отчетности и времени отчетности; эти показатели следует рассматривать вместе, а не по отдельности, поскольку раннее сообщение может значительно улучшить усилия по смягчению последствий. Являются ли показатели отчетности выше, чем показатели кликов? Время для первого отчета раньше, чем время для первого клика?

Мы надеемся организовать дискуссию о высоких показателях кликов таким образом, чтобы это имело смысл для директоров по информационной безопасности, и утверждаем, что высокие показатели кликов могут указывать на то, что пользователи подвергаются новым, сложным и контекстуально релевантным фишинговым кампаниям. Мы твердо верим, что сложные упражнения, являющиеся частью комплексной программы кибербезопасности для повышения осведомленности о фишинге, на самом деле повышают эффективность обучения пользователей и осведомленность о реальных угрозах, а не просто повторяют одни и те же или очень похожие фишинговые сообщения, которые легче обнаружить. Рейтинг кликов следует рассматривать в сочетании с более глубоким пониманием самих фишинговых писем, а также в свете поведения отчетов. С этой целью мы разработали шкалу фишинга, чтобы помочь директорам по информационной безопасности лучше понять и охарактеризовать сложность обнаружения конкретного действия по фишингу. Используя оперативные данные, Шкала указывает на трудности, с которыми пользователи электронной почты в целевой группе могут столкнуться при обнаружении конкретного фишингового сообщения. Шкала фишинга учитывает несколько компонентов сложности обнаружения фишинга: подсказки, такие как ссылки [15 ] и [ 16 ] и выравнивание пользовательского контекста [ 3 ].

Хотя наш список сигналов Phish Scale довольно обширен, он не является исчерпывающим; однако разработчики фишинговых сообщений постоянно совершенствуют свои методы, и список подсказок легко расширяется. При переходе к более шаблонному подходу к категоризации выравнивания предпосылок (метод 2), чем представленный в исх. [ 18 ], теперь мы включаем измерения воспринимаемой серьезности последствий и тренировочных эффектов. Грин и др . . [ 3 ] обнаружили, что кликеры были обеспокоены последствиями, возникающими из -защелчки, например, неспособность реагировать на свои рабочие обязанности. Напротив, те, кто не кликал, были больше обеспокоены последствиями кликов, например, случайной загрузкой вредоносного ПО. Кроме того, опасения по поводу последствий варьировались в зависимости от предпосылки фишинга. Например, вполне вероятно, что опасения по поводу последствий были намного выше для упражнения Weblogs с его подразумеваемым следствием дисциплинарных мер, включая увольнение. Мы считаем, что добавление более шаблонного подхода к категоризации соответствия предпосылкам, который включает элементы: ( i) имитирует практику или практику на рабочем месте, (ii) имеет отношение к рабочему месту, (iii) согласуется с другими ситуациями или событиями, (iv) вызывает озабоченность по поводу отказ от кликов и (v) целевое обучение, конкретные предупреждения и другое воздействие,упростить для директоров по информационной безопасности и специалистов по обучению категоризацию согласования предпосылок.

Мы ожидаем, что три определенных нами рейтинга сложности обнаружения — « Очень сложно» , «Умеренно сложно » и «Наименее сложно» — в конечном итоге будут соответствовать проверенным диапазонам рейтинга кликов. Говоря с директорами по информационной безопасности, мы предполагаем диапазоны примерно в следующем порядке: очень сложная категория, имеющая рейтинг кликов около или выше 20%, умеренно сложная категория, имеющая рейтинг кликов в диапазоне примерно от 10 до 20%, и наименее сложная категория, имеющая рейтинг кликов. ниже 10%. Мы планируем информировать фактические диапазоны дополнительными эмпирическими данными; десять упражнений, представленных здесь, являются началом.

Тем не менее, шкала Phish находится на ранней стадии, но мы считаем, что концептуальная основа многообещающая, если принять во внимание прогнозируемый рейтинг сложности обнаружения и фактическую частоту кликов для десяти изученных нами упражнений. Кроме того, мы подчеркиваем, что компоненты Phish Scale все еще находятся в разработке. Мы знаем, что все сигналы не имеют одинаковой значимости. Найти сокращенный метод для CISO, чтобы охарактеризовать согласованность предпосылок, оказалось непросто. Тем не менее, мы считаем, что есть смысл разделить сложность обнаружения фишинговых сообщений, чтобы адаптировать обучение и контекстуализировать частоту кликов как для обучения, так и для реальных угроз.

Дифференциальная значимость сигнала: не все сигналы созданы одинаково

Зафиксировать эффект подсказок фишинговых сообщений сложно, так как не все подсказки создаются одинаково. Заметность и эффект любого конкретного фишингового сигнала различаются в зависимости от того, воспринимается ли он как индикатор подозрения или убедительный крючок. Важно отметить этот аспект характеристик фишинговых сообщений. Воспринимается ли подсказка как индикатор фишинга или ловушка, зависит от пользователя и контекста пользователя при обработке электронной почты. Хорошо известные индикаторы фишинга, такие как орфографические и грамматические ошибки, часто рассматриваются пользователями электронной почты как вызывающие подозрения, и их обнаружение может привести к дополнительному изучению сообщения пользователями на наличие дополнительных индикаторов фишинга. Еще одной бесспорной характеристикой фишинга является срочность. Его использование настолько распространено, что это должно быть красным флажком; тем не менее, срочность является обычным явлением в современном мире, ослабляя мощность сигнала, вызывающего подозрения. Кроме того, срочность тормозит более медленные, более обдуманные действия (Система 2 [[Система 2]).12 ]), что делает его скорее усилителем крючка, чем красным флажком.

Мы подозреваем, что значимость некоторых сигналов может на самом деле отражаться в категоризации выравнивания предпосылок. Например, в упражнении «Неоплаченный счет» обозначение отправителя как (Fed) в поле «От» сообщения служило убедительным сигналом для тех, кто щелкнул мышью, поскольку это имитировало принятое на рабочем месте соглашение и практику. Присутствие этого элемента сообщения усилило общую согласованность предпосылок и, таким образом, повысило категоризацию согласованности предпосылок.

Категоризация предпосылок в соответствии с пользовательским контекстом

В этой ранней версии шкалы фишинга мы используем термины « высокий », «средний » и « низкий» , чтобы разделить предпосылки для целевой аудитории на интуитивно понятные категории высокого уровня с соответствующими определениями (метод 1). В этой работе документирован более шаблонный подход: категоризация выравнивания предпосылок (Метод 2). Хотя этих методов достаточно для начального этапа разработки шкалы, мы можем попытаться усовершенствовать методы характеристики категориальных переменных в будущей работе, исследуя меры и шкалы контекстуальной релевантности. «Контекстный» является частью существующих шкал в других областях, таких как «Контекстная мера мотивации достижения» [ 40 ] и «контекстная производительность» как измерение индивидуальной производительности труда [40].41 ]. Как можно использовать такие существующие шкалы и меры для использования в области фишинга? Кроме того, как мы учитываем изменения контекста с течением времени?

Изменения в контекстуальной релевантности могут происходить в течение довольно длительного периода времени, когда кто-то медленно добавляет или меняет должностные обязанности в течение многих лет своей карьеры, или очень коротких временных масштабов, поскольку какое-то событие в этот день/неделю/месяц может вызвать повышенную контекстуальную релевантность. Например, Грин и др . [ 3] объяснил, что пользователи были обеспокоены неоплаченным счетом-фактурой реального поставщика, что привело к временной повышенной контекстуальной релевантности фишингового электронного письма с неоплаченным счетом-фактурой. Ежедневные события, такие как ожидание или отсутствие телефонного звонка, могут временно повысить контекстуальную релевантность фишингового электронного письма с «новой голосовой почтой». Такие факторы, как занятость, стресс или спешка, также могут сильно колебаться в течение рабочего дня. Вполне вероятно, что существует относительно фиксированный компонент пользовательского контекста в дополнение к более чувствительному ко времени переменному компоненту. Текущая шкала Phish не разбивает контекст и связанное с ним выравнивание предпосылок на эти подкомпоненты. Неясно, действительно ли необходимо такое тонкое разграничение на данном этапе.

Хотя может быть вполне осуществимо различить соответствие предпосылкам с большей детализацией, чем наши существующие категории, на самом деле это может быть излишним для предполагаемой аудитории шкалы Phish. С нашей целью разработать простую, удобную в использовании шкалу фишинга для директоров по информационной безопасности и лиц, ответственных за реализацию и контроль учебных программ по осведомленности о фишинге, вполне вероятно, что высокий , средний и низкийкатегорий для выравнивания предпосылок достаточно. Важный момент, который мы стремимся подчеркнуть с помощью нашей шкалы фишинга, заключается в том, что в очень релевантном контексте пользователям чрезвычайно сложно обнаружить фишинговые электронные письма. Чем выше контекстуальная релевантность, тем меньше вероятность того, что пользователь заметит подозрительные сообщения электронной почты, проявит внимание и глубоко обдумает их. Ежедневные стрессовые факторы, такие как нехватка времени, в целом сокращают когнитивные ресурсы, которые пользователи могут использовать для обработки электронной почты. Когда когнитивные ресурсы сокращаются, повышается вероятность того, что пользователи будут заниматься более быстрой, эвристической обработкой в ​​Системе 1, а не вдумчивой, более медленной и глубокой обработкой в ​​Системе 2 [12 ] .

И последний момент, касающийся пользовательского контекста и выравнивания предпосылок, связан с размером целевой аудитории: категоризировать выравнивание предпосылок становится все труднее по мере увеличения размера целевой аудитории. При более широкой целевой аудитории обычно присутствует гораздо большее разнообразие рабочих обязанностей и более широкий спектр пользовательских контекстов, которые могут соответствовать или не соответствовать предпосылке фишинговой электронной почты. В зависимости от предпосылки фишингового сообщения может оказаться полезным дополнительный анализ рейтинга кликов для групп на основе рабочих ролей, а не для большой целевой аудитории с разными ролями. В любом случае выравнивание посылок должно определяться кем-то, кто хорошо разбирается в коллективном контексте работы с конкретной целевой аудиторией фишингового сообщения. Чтобы иметь смысл, иначе и быть не может.

Сравнение данных о фишинге по секторам

Несмотря на то, что часто проводятся межотраслевые и межсекторальные сравнения фишинговых атак, интерпретация таких сравнений по-прежнему сопряжена со значительными трудностями. В частности, когда уровень сложности обнаружения фишинга может так сильно различаться в зависимости от пользовательского контекста и предпосылок, это в некотором смысле бессмысленное сравнение без базового понимания и оценки: (i) характеристик самого фишингового электронного письма и (ii ) характеристики целевой группы пользователей. В частности, необходимо понимать предпосылки и сигналы, содержащиеся в данном фише, в сочетании с рабочим контекстом целевой группы пользователей. С этой целью мы считаем, что наша шкала фишинга показывает большие перспективы в качестве инструмента, помогающего организовать обмен данными о частоте кликов и отчетах по упражнениям, организациям и секторам.

По мере того, как мы совершенствуем и совершенствуем этот инструмент при участии более широкого сообщества специалистов по безопасности, мы надеемся вывести Phish Scale из исследовательского сообщества в область оперативного использования. Например, мы считаем, что помимо преимуществ для директоров по информационной безопасности и специалистов по обучению фишингу, наша шкала фишинга также может принести значительную пользу совместным организациям, ответственным за обмен данными разведки о киберугрозах. Например, Федеральное бюро расследований (ФБР) имеет программу InfraGard, партнерство между ФБР и частным сектором, предназначенное для обмена информацией и разведывательными данными [ 42] .]. Существуют и другие подобные совместные программы, например, Национальный альянс по киберкриминалистике и обучению (NCFTA), который представляет собой некоммерческое партнерство между частным сектором, правительством и академическими кругами, работающими вместе для борьбы с киберпреступностью [ 43 ] . Фишинг в частности и социальная инженерия в целом представляют собой активные угрозы во всех отраслевых вертикалях. Предоставляя структуру оценки сложности фишинга, наша шкала фишинга может помочь облегчить совместную работу, используя общий язык, связанный с обнаружением угроз фишинга людьми.

Будущая работа

Мы призываем других полезных исследователей и практиков в области безопасности использовать нашу шкалу фишинга, применять ее к гораздо более широкому спектру фишинговых электронных писем и проверять ее прогнозы как на существующих данных учебных упражнений по фишингу, так и, в конечном счете, на реальных фишинговых электронных письмах. Мы планируем продолжать применять нашу шкалу фишинга к большему количеству дополнительных электронных писем, для которых у нас есть данные о рейтинге кликов и выравнивании предпосылок, и планируем сотрудничать с внешними организациями, чтобы сделать то же самое. К сожалению, наш доступ к одновременным данным отчетов более ограничен. Заметная проблема проведения исследований с оперативными данными о рабочих местах заключается в том, что часто приходится идти на компромисс между экспериментальным контролем и экологической достоверностью. В этом случае мы имели преимущество чрезвычайно высокой экологической достоверности, поскольку пользователи находились в своих обычных рабочих условиях со своими обычными задачами и загрузкой электронной почты, но без контроля, необходимого для сбора отчетов о количестве сообщений во время фишинговых упражнений. Тем не менее, преимущество наличия новых,данные о рабочих местах примерно 5000 сотрудников являются важным вкладом в литературу по фишингу и в более широкое полезное сообщество по безопасности.

Помимо применения и тестирования текущей шкалы Phish с дополнительными данными, мы также намерены изучить новые компоненты шкалы. Мы хотели бы исследовать включение работы над личностными факторами, любопытством, рассеянностью, заботой о безопасности и, в конечном итоге, сведением различных компонентов нашей шкалы Phish в модель линзы, приложение множественной регрессии, часто используемое в исследованиях суждения и принятия решений. Это будет основано на предыдущей работе Тамборелло и Грина по моделированию линз [ 44 ], а также Молинаро и Болтона [ 15] .]. Дополнительные исследования моделирования и симуляции могут изучить прогнозируемую частоту кликов и частоту сообщений для различных комбинаций сигналов, согласования контекста, типов личности и предпосылок фишинга. Как различные комбинации влияют на восприимчивость к фишингу? Например, рассмотрите эту комбинацию: пользователи с высокими баллами по добросовестности, с контекстом финансовой работы, которые получают фишинговое электронное письмо с авторитарным/срочным переводом средств, и очень мало подозрительных сигналов. Что, если бы все было таким же, кроме рабочего контекста, достаточно ли одной этой разницы, чтобы кто-то поймал этот фишинг? Хотя мы считаем, что контекст может преобладать над всем, необходимы дополнительные исследования, чтобы увидеть, в каких сценариях это происходит, а также как и когда это может измениться.

Более широкие последствия

Шкала фишинга — да и фишинга в целом — является частью гораздо более широкой исследовательской программы, направленной на решение целого ряда полезных вопросов безопасности. Например, понимание риска, в том числе человеческого риска, является ключевым компонентом стратегии кибербезопасности любой организации, а системы управления рисками играют важную роль в поддержании безопасности и конфиденциальности [ 45] .]. В конечном счете, мы надеемся, что наша шкала фишинга может быть использована для того, чтобы помочь директорам по информационной безопасности лучше понять и охарактеризовать риск фишинга в их организации, по сути профилируя типы предпосылок фишинга, которым более или менее подвержены их пользователи, а также фактические угрозы организации. Такие данные можно использовать для приоритизации усилий по обучению более целенаправленным вмешательствам, а также для приоритизации усилий по расследованию подозреваемых фишинговых атак в реальном мире. Целевые обучающие вмешательства, вероятно, должны будут выйти за рамки встроенных упражнений по фишингу, особенно для повторяющихся кликеров. Личные семинары, плакаты, неформальные обеды и учебные занятия и т. д. — все это часть более крупной программы повышения осведомленности о безопасности. Дополнительные вмешательства могут включать специальные элементы графического пользовательского интерфейса (GUI) электронной почты или пометки,

В дополнение к профилированию рисков и целевому обучению в будущем также необходимо понять, как новые технологические меры безопасности электронной почты повлияют на фишинг. В частности, государственные учреждения быстро переходят к аутентификации электронной почты, внедряя такие протоколы, как аутентификация сообщений на основе домена, отчетность и соответствие (DMARC) и почта с идентификацией ключей домена (DKIM) в соответствии с обязательной операционной директивой 18 Министерства внутренней безопасности (DHS). -01 [ 46]. Как это повлияет на фишинговое пространство? С другой стороны, использование предтекстов уже набирает популярность и, вероятно, продолжит набирать популярность, особенно если новые технологические решения предотвращают или угрожают успеху некоторых более «традиционных» фишинговых электронных писем. По мере того, как достижения в области технологий защиты делают некоторые атаки менее эффективными или даже устареют на один день, атаки не прекратятся, а скорее изменятся и будут развиваться в ответ. Например, вполне вероятно, что другие внеполосные методы социальной инженерии будут продолжать набирать популярность. Фишинг — лишь один из компонентов гораздо более крупной проблемы социальной инженерии, с которой сталкивается область кибербезопасности. Будущая работа должна изучить, как уроки, извлеченные в области фишинга, могут также повлиять на другие разновидности проблем социальной инженерии.

использованная литература

1 Предприятия кибербезопасности.2019Отчет о киберпреступлениях, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (15 мая 2020 г., дата последнего доступа).

2 Грин КК,Стивс М,Феофанос М. Никакого фишинга после этой точки. ВКолонка IEEE Comp Cybertrust 2018;51:86–89.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

3 Грин КК,Стивс М,Феофанос Ми другие. Контекст пользователя: пояснительная переменная в восприимчивости к фишингу. USEC NDSS 2018. Практический семинар по безопасности на симпозиуме по безопасности сетей и распределенных систем. 18 февраля2018. Сан-Диего, Калифорния. DOI: https://dx.doi.org/10.14722/usec.2018.23016

4 Новый человек ЛХ.Что спамеры могут сделать с вашими взломанными данными Facebook. проводной ,2018, https://www.wired.com/story/facebook-hack-data-spammers/ (май 2020 г., дата последнего доступа).

5 Ежегодная конференция Healthcare CyberGard, Шарлотта, октябрь2018, https://www.ncfta.net/healthcare-cybergard-annual-conference-charlotte-october-2018/ (май 2020 г., дата последнего доступа).

6 Консультативный совет по информационной безопасности и конфиденциальности, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/minutes/ispab-june-2018-meeting-minutes.pdf (май 2020 г., дата последнего доступа).

7 Сойер БД,Хэнкок ПА. Взлом человека: парадокс распространенности в кибербезопасности.Человеческие факторы 2018;60:597–609.

Google ученыйперекрестная ссылка Найдите в моей библиотеке пабмедWorldCat

8 Левари DE,Гилберт ДТ,Уилсон ТДи другие. Изменение концепции человеческого суждения, вызванное преобладанием.Наука 2018;360:1465–7.

Google ученыйперекрестная ссылка Найдите в моей библиотеке пабмедWorldCat

9 Роджерс РВ. Теория защитной мотивации призывов к страху и изменения отношения.Джей Психол 1975 г.;91:93–114.

Google ученыйперекрестная ссылка Найдите в моей библиотеке пабмедWorldCat

10 Ван Дж,Ли Д,Рао Р. Реакция на обнаружение фишинга: исследование предпосылок и последствий.Инф Сист Рес 2017;28:378–96.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

11 Вишванатх А,Херат Т,Чен ри другие. Почему люди становятся жертвами фишинга? Тестирование индивидуальных различий в уязвимости к фишингу в рамках интегрированной модели обработки информации.Децис Supp Syst 2011;51:576–86.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

12 Канеман Д. Мышление, быстрое и медленное.Нью-Йорк:Фаррар, Штраус и Жиру,2011.

Google ученыйПредварительный просмотр GoogleНайдите в моей библиотекеWorldCatКОПАК

13 Вишванатх А,Харрисон Б,Нг Й.Дж. Подозрение, распознавание и автоматическая модель восприимчивости к фишингу.Связь Res 2018;45:1146–66.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

14 Уильямс ЭДж,Хиндс Дж,Джойнсон АН. Изучение подверженности фишингу на рабочем месте.Int J Human-Comp Stud 2018;120:1–13.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

15 Молинаро КА,Болтон мл. Оценка применимости модели двойной системы линз к анализу суждений о фишинговых электронных письмах.Комп сек. 2018;77:128–37.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

16 Парсонс К,Бутавичюс М,Паттинсон Ми другие. Сосредоточены ли пользователи на правильных признаках, позволяющих отличить фишинговые сообщения от настоящих?.Австралазийская конференция по информационным системам 2015; https://arxiv.org/abs/1605.04717 (май 2020 г., дата последнего доступа).

Google ученыйНайдите в моей библиотекеWorldCat

17 Капуто Д,Пфлегер СЛ,Фриман Джи другие. Целевой фишинг: знакомство со встроенным обучением и повышением осведомленности.IEEE Sec Priv 2014;12:28–38.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

18 Стивс М,Грин К,Феофанос М.Шкала фишинга: оценка сложности обнаружения фишинговых сообщений от людей. USEC NDSS 2019. Практический семинар по безопасности на симпозиуме по безопасности сетей и распределенных систем . февраль,2019. Сан-Диего, Калифорния. DOI: https://dx.doi.org/10.14722/usec.2019.23028 .

19 Блайт М,Петри ЧАС,Кларк Дж.А.F — подделка: четыре исследования о том, как мы попадаемся на фишинг. В: Материалы конференции SIGCHI по человеческому фактору в вычислительных системах, май 2011 г. , Ванкувер, Канада, ACM.2011, стр.3469–78.

20 Кэнфилд КИ,Фишхофф Б,Дэвис А. Количественная оценка восприимчивости к фишингу для обнаружения и принятия решений о поведении.Человеческий факт 2016;58:1158–72.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

21 Даунс JS,Холбрук М,Кранор ЛФ. Стратегии принятия решений и подверженность фишингу . В: Материалы второго симпозиума по полезной конфиденциальности и безопасности (SUPS '06), ACM,2006 г., стр.79–90.

22 Фернелл С. Фишинг: можем ли мы обнаружить признаки? Секунда мошенничества с комп. 2007 г.;2007 г.:10–15.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

23 Грациоли С. Где они ошиблись? Анализ неспособности осведомленных интернет-потребителей обнаружить обман в Интернете.Группа Децис Негот 2004 г.;13:149–72.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

24 Хаднадь С,Финчер М. Фишинг Темные воды. Хобокен, Нью-Джерси:Уайли,2015.

Google ученыйперекрестная ссылка Найдите в моей библиотеке Предварительный просмотр GoogleWorldCatКОПАК

25 Якобссон М. Человеческий фактор в фишинге.Информация о потреблении конфиденциальной информации 2007 г.;7:1–19.

Google ученыйНайдите в моей библиотекеWorldCat

26 Якобссон М,Финн П.Планирование и проведение фишинговых экспериментов. В: Журнал IEEE Technology and Society, специальный выпуск по удобству использования и безопасности , IEEE,2007 г..

27 Каракасилиотис А,Фернелл С,Пападаки М.Оценка осведомленности конечных пользователей о социальной инженерии и фишинге. В: Австралийская конференция по информационной войне и безопасности , Школа компьютерных и информационных наук,2006 г., Университет Эдит Коуэн, Перт, Западная Австралия.

28 Парсонс К,МакКормак А,Паттинсон Ми другие. Фишинг ради правды: основанный на сценариях эксперимент по поведенческой реакции пользователей на электронные письма. В:Международная конференция по информационной безопасности IFIP,Спрингер,Берлин, Гейдельберг,2013, стр.366–78.

Google ученыйПредварительный просмотр GoogleНайдите в моей библиотекеWorldCatКОПАК

29 Ван Дж,Херат Т,Чен ри другие. Подверженность фишингу: расследование обработки целевого фишингового письма. IEEE Trans Prof Comm 2012;55;345–62.

30 Райт р,Чакраборти С,Басоглу Аи другие. 'Куда они пошли прямо? Понимание обмана в фишинговых сообщениях.Группа Децис Негот 2010;19:391–416.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

31 Хан Д,Шен Ю.Точная атрибуция целевого фишинга и раннее обнаружение. В: Материалы 31-го ежегодного симпозиума ACM по прикладным вычислениям , ACM,2016, стр.2079–86.

32 Ким Д,Ким Дж. Х. Понимание элементов убеждения в фишинговых электронных письмах: категориальное содержание и анализ семантической сети.Онлайн Информ Рев. 2013;37:835–50.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

33 Эгельман С,Кранор НЧ,Хонг Дж.Вас предупредили: эмпирическое исследование эффективности предупреждений о фишинге в веб-браузере. В материалах конференции SIGCHI по человеческому фактору в вычислительных системах , ACM,2008 г., стр.1065–74.

34 Цоу А,Якобссон М.Обман и обман: большое пользовательское исследование фишинга. Университет Индианы, Технический отчет TR649,2007 г..

35 Дхамиджа р,Тайгар Джей Ди,Херст М.Почему фишинг работает. В: Материалы конференции SIGCHI по человеческому фактору в вычислительных системах , ACM,2006 г., стр.581–90.

36 Фогг БЖ.Теория известности-интерпретации: объяснение того, как люди оценивают доверие в Интернете. В CHI'03 Extended Abstracts on Human Factors in Computing Systems , ACM,2003 г., стр.722–23.

37 Алшарноуби М,Алака Ф,Чиассон С. Почему фишинг все еще работает: пользовательские стратегии борьбы с фишинговыми атаками.Int J Human-Comp Stud 2015;82:69–82.

Google ученыйперекрестная ссылка Найдите в моей библиотеке WorldCat

38 Перкинс Д,Саломон ГРАММ. Передача обучения.Инт Энцикл Эду 1992 г.;2:6452–57.

Google ученыйНайдите в моей библиотекеWorldCat

39 Программа-вымогатель, https://www.trendmicro.com/vinfo/us/security/definition/RANSOMWARE (май 2020 г., дата последнего доступа).

40 Смит РЛ.Контекстная мера мотивации достижения: значение для исследований в области консультирования. ВИЗИТ онлайн ,2015.

41 Купманс л,Бернаардс СМ,Гильдебрандт ВХи другие. Измерение индивидуальной эффективности работы: определение и выбор показателей.Работа 2014;48:229–38.

Google ученыйперекрестная ссылка Найдите в моей библиотеке пабмедWorldCat

42 ФБР, Федеральное бюро расследований. https://www.fbi.gov/about/partnerships/infragard (май 2020 г., дата последнего доступа).

43 NCFTA, Национальный альянс киберкриминалистики и обучения, https://www.ncfta.net . (май 2020 г., дата последнего доступа).

44 Тамборелло ФП,Грин КК.Исследовательская линзовая модель принятия решений в потенциальном сценарии фишинговой атаки. Межведомственный отчет Национального института стандартов и технологий, NISTIR 8194, октябрь2017. https://doi.org/10.6028/NIST.IR.8194 .

45 NIST, Национальный институт стандартов и технологий, «Специальная публикация 800-37, редакция 2, Структура управления рисками для информационных систем и организаций — подход к обеспечению безопасности и конфиденциальности на основе жизненного цикла системы»,2018.

46 DHS, Министерство внутренней безопасности. Обязательная операционная директива BOD-18-01, 2017 г., https://cyber.dhs.gov/assets/report/bod-18-01.pdf (май 2020 г., дата последнего доступа).

Опубликовано издательством Oxford University Press в 2020 г. Эта работа написана служащими правительства США и находится в общественном достоянии США.

Эта статья публикуется и распространяется на условиях издательства Oxford University Press, Standard Journals Publication Model ( https://academic.oup.com/journals/pages/open\_access/funder\_policies/chorus/standard\_publication\_model )

Опубликовано издательством Oxford University Press в 2020 г. Эта работа написана служащими правительства США и находится в общественном достоянии США.