Международный союз электросвязи

МСЭ-Т X.1212

(03/2017)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности

Рекомендация МСЭ-Т X.1212

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных системы (ИТС)	X.1370–X.1379
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1212

Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности

Резюме

В разнообразных видах атак используется контент, скопированный у заслуживающих доверие поставщиков услуг, что вводит в заблуждение конечных пользователей, заставляя их поверить в ложную благонадежность этого контента.

В Рекомендации МСЭ-Т X.1212 представлены проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности. В дополнениях описываются типичные методы измерения восприятия конечным пользователем таких показателей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1212	30.03.2017 г.	17-я	11.1002/1000/13195

Ключевые слова

Восприятие конечным пользователем, фишинг, показатели благонадежности.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1212

Проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности

1 Сфера применения

В разнообразных видах атак используется контент, скопированный у заслуживающих доверие поставщиков услуг, что вводит в заблуждение конечных пользователей, заставляя их поверить в ложную благонадежность этого контента. В Рекомендации МСЭ-Т представлены проектные решения для улучшенного восприятия конечным пользователем показателей благонадежности. В дополнениях описываются типичные методы измерения восприятия конечным пользователем таких показателей.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 ограниченные возможности (disability) [b-ITU-T F.790]: Это понятие определяется как состояние, когда ограничены возможности использования оборудования и услуг электросвязи. Обычно считается, что "ограниченные возможности" являются результатом временного или постоянного ограничения физических возможностей из-за болезни, аварии, старости и т. д. В более общем смысле понятие "ограниченные возможности" включает в себя состояние, когда полное использование оборудования и услуг связи невозможно из-за физических или социальных условий (например, голосовая телефония в условиях высокого уровня шумов).

3.1.2 измерение (measurement) [b-ENISA]: Действие по измерению или процесс измерения, при котором определяется значение количественной переменной в сравнении со (стандартной) единицей измерения.

3.1.3 метрика (metric) [b-ENISA]: Система связанных измерений, позволяющих получить количественное выражение некоторых характеристик системы, компонента или процесса. Метрика состоит из двух или более мер.

3.1.4 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ITU-T X.1252]: Любая информация, a) которая идентифицирует или может использоваться для идентификации, обращения или установления местоположения лица, к которому такая информация относится; b) на основе которой может быть осуществлена идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

3.1.5 фишинг (phishing) [b-ITU X.1254]: Мошенничество, при котором пользователь электронной почты или веб обманом вынуждается раскрыть личную или конфиденциальную информацию, которую мошенник затем может незаконно использовать.

3.1.6 доступность электросвязи (telecommunications accessibility) [b-ITU-T F.790]: Для сферы электросвязи – это возможность использования продукта, услуг, среды передачи или оборудования наиболее широким кругом пользователей и особенно пользователей с ограниченными возможностями.

3.1.7 лицо с ограниченными возможностями (person with disabilities) [b-ITU-T F.791]: Корректное именование лица с инвалидностью [b-UNCRPD].

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин:

3.2.1 показатели благонадежности (trustworthiness indicators): Символы, представленные агентом пользователя веб, которые будут применяться для информирования конечных пользователей о благонадежности веб-сайта.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

DKIM	DomainKeys Identified Mail	Идентификация почты с использованием доменных ключей
DOM	Document Object Model	Объектная модель документов
FNE	Fear of Negative Evaluation	Боязнь негативной оценки
SSL	Secure Socket Layer	Уровень защищенных сокетов
URL	Uniform Resource Locator	Универсальный указатель ресурса

5 Условные обозначения

Отсутствуют.

6 Восприятие конечным пользователем показателей благонадежности

Протоколы обмена информацией о кибербезопасности, определенные в [b-ITU-T X.1500], могут содержать полезную информацию для принятия решений о степени доверия к любым взаимодействиям в киберпространстве. Такая информация включает, в том числе, информацию о сертификатах с расширенной валидацией [b-CAB-Baseline], уровне гарантии идентичностей [b-ITU-T X.1254], подписях для идентификации почты с использованием доменных ключей (DKIM) в электронной почте [b-IETF RFC 6376] и об индикации фишинг-сайтов [b-IETF RFC 5901].

Однако эти показатели благонадежности часто игнорируются или в крайне малой степени учитываются конечными пользователями, как показали последние исследования, основанные на разнообразных демографических показателях (более подробная информация представлена в Дополнении II). Вследствие этого необходимо улучшить восприятие конечным пользователем показателей благонадежности.

7 Методы обеспечения улучшенного восприятия конечным пользователем показателей благонадежности

В этом разделе представлены несколько методов улучшения восприятия конечным пользователем показателей благонадежности. Эти методы могут использоваться индивидуально или в комбинации, в зависимости от желания или необходимости, для представления показателей благонадежности в более узнаваемом виде.

7.1 Визуальные элементы

Разработчики показателей благонадежности должны учитывать использование стандартизованных визуальных элементов. Проведенные в прошлом исследования показали, что представление показателей благонадежности в символьном виде, например, в универсальных указателях ресурсов (URL), неудобно для неопытных пользователей, которые их часто игнорируют [b-Miyamoto]. Поэтому рекомендуется внедрять визуальные элементы, например, значки, отображающие показатели благонадежности. Разработчики могут рассмотреть возможность применения небольшого количества стандартных визуальных элементов типа дорожных знаков, с целью свести к минимуму вспомогательную информацию, необходимую для восприятия и обучения.

В соответствии с правилами применения знаков и маркировки продукции [b-ANSI-Z535.4], использование сигнализирующих слов (например, "Опасно", "Внимание"), выделенных соответствующим цветом (красный, оранжевый, желтый), уменьшает уровень рисков.

Рисунок 1 – Знаки и маркировка безопасности продукции (ANSI Z535.4)

В сообщении "ОПАСНО" используется белый треугольник с красным восклицательным знаком, расположенный на красном фоне. В сообщении "ПРЕДОСТЕРЕЖЕНИЕ" используется черный треугольник с оранжевым восклицательным знаком. В сообщении "ОСТОРОЖНО" используется черный треугольник с желтым восклицательным знаком.

Кроме того, тем, кто внедряет показатели благонадежности, следует применять стандартные схемы цветового оформления для отображения уровня доверия. С точки зрения психологии воздействия цвета красный цвет используется для привлечения внимания. У красного цвета самая большая длина волны в спектре видимого света, которая придает предметам свойство казаться ближе, чем на самом деле. Поэтому красный цвет захватывает внимание пользователей и используется в дорожных светофорах. У желтого цвета относительно большая и довольно стимулирующая длина волны, и он привлекает внимание пользователей. Зеленый цвет находится в центре видимого спектра и характеризуется промежуточным значением длины волны. Зрению не нужно приспосабливаться к зеленому цвету, поэтому он используется в успокаивающих и снижающих тревогу знаках. Голубой цвет успокаивает сознание и способствует концентрации.

Разработчики показателей благонадежности могут использовать концепцию "социального мышления", поощряющую поведение в интересах общества и сотрудничества. Последние исследования показали, что люди ведут себя более социально осознанным образом, когда рядом с ними находятся изображения наблюдающих глаз [b-Rigdon, b-Senju]. В отношении этого имеется и скептическое мнение, согласно которому изображение наблюдающих глаз оказывает небольшое влияние или не оказывает никакого влияния на поведение [b-Felt2014].

7.2 Описательные элементы

Последние исследования показали, что определенные группы пользователей принимают решения о благонадежности, основываясь на описательных надписях, а не наименованиях доменов, типах протоколов или URL [b-Felst2014], [b-Felt2015]. Рекомендуется оснащать программное обеспечение конечных пользователей функцией преобразования символической информации в описательные элементы, в которых не применяются сокращения. Это может быть полезно в случае пользователей с нарушениями зрения, если такие элементы применять в сочетании с системами преобразования текста в речь.

Для того, чтобы привлечь внимание пользователей, например, предостерегающими сообщениями, при разработке программного обеспечения конечных пользователей может потребоваться рассмотреть применение ряда следующих критериев проектирования:

1) Разработчикам показателей благонадежности следует избегать использования технических терминов. В предостерегающих сообщениях технические термины следует заменять фразами и выражениями, которые могут быть понятны пользователям – они будут игнорировать сообщения, если не будут знать, как правильно на них реагировать.

2) Разработчикам показателей благонадежности следует учитывать краткость сообщений. Большой объем текста будет указывать на то, что для его прочтения потребуется много усилий, поэтому пользователи не станут читать его. Избыточный текст следует убрать из сообщения, чтобы оно было кратким и точным. Следует отметить, что необходимо соблюдать компромисс между краткостью и точностью: невозможно объяснить все аспекты модели угрозы в единственном коротком абзаце. Следовательно, в предостерегающих сообщениях могут использоваться как визуальные, так и текстовые элементы. Чтобы рассчитать уровень краткости, разработчики могут применить индекс удобочитаемости, который является мерой удобочитаемости, оцениваемой количеством лет образования, необходимых человеку для понимания написанного абзаца.

3) Разработчикам показателей благонадежности следует описывать то рискованное событие, которое случилось или может случиться. В предостерегающих сообщениях следует описывать риск, лежащий в основе события, поскольку пользователи скорее поймут и будут реагировать на сообщение, если оно описывает риск наступления события точно и недвусмысленно. Сообщение должно также содержать инструкции о том, как избежать риска, если только эти инструкции не являются очевидными из формулировки риска.

7.3 Проектирование периферийных переходов

Разработчики показателей благонадежности могут проверить их интерфейс в отношении проектирования периферийных переходов. Внезапные переходы в области периферийного зрения могут эффективно сигнализировать о потенциальном риске. Поэтому рекомендуется применять этот метод путем изменения периферийной области экрана (обычно называется "темой" или "скином"), когда конечный пользователь сталкивается с веб-сайтами или сообщениями электронной почты, обладающими высокой степенью риска.

7.4 Режим обучения

Разработчики показателей благонадежности могут подготовить режимы обучения. Восприятие риска конечным пользователем в лучшем случае будет неточным, если он/она редко подвергается таким рискам. Поэтому рекомендуется встроить в программное обеспечение конечного пользователя режим обучения, в котором искусственно будет генерироваться наступление смоделированных рискованных событий, и конечный пользователь будет обучаться точности их восприятия. Такое обучение может стимулироваться игровым представлением процесса обучения.

7.5 Доступность

Разработчикам показателей благонадежности следует проектировать интерфейс с учетом доступности. Зрительное восприятие подразумевает способность различать вид, размер, форму и цвет визуальных раздражителей. У лиц с ограниченными возможностями по зрению могут возникнуть трудности в нахождении показателей благонадежности. Вследствие эффектов, известных под названиями "протанопия" (отсутствие восприятия красного цвета) и "дейтеранопия" (отсутствие восприятия зеленого цвета) у некоторых конечных пользователей могут возникнуть проблемы с различением цветов, например, отличить красный цвет от зеленого.

ИСО/МЭК разработали документ, содержащий руководящие указания по доступности для лиц с ограниченными возможностями [b-ISO/IEC 40500], хотя в нем непосредственно не рассматриваются показатели благонадежности в адресной строке. В документе Браузерного форума СА по базовым требованиям [b-CAB-Baseline] определяется стандарт на сертификаты и органы сертификации, хотя в нем не определяется, как браузеры будут представлять пользователям эти сертификаты.

В контрольном перечне по вопросам доступности электросвязи [b-ITU-T-FSTP-TACL] гарантируется доступность конкретных услуг и функций для различных групп пользователей, включая лиц с ограниченными возможностями. Для того, чтобы обеспечить лучшую доступность для лиц с ограниченными возможностями по зрению или слепых, в интерфейсе следует предусмотреть для

пользователей мультимедийное представление, а также возможность осуществления управления при различных режимах и видах управляющих действий. Для привлечения внимания лиц с нарушением когнитивных способностей следует выделять важные моменты, используя в том числе дополнительные средства информации, такие как пиктограммы, видео- и аудиоматериалы.

Приложения для чтения экрана могут извлекать показатели благонадежности из веб-сайтов. Они могут отображать информацию о безопасности, например, адресную строку зеленого цвета в сертификате EV-SSL, и считывать информацию с помощью услуг преобразования текста в речь. Они также могут извлекать итоговую информацию из дерева объектной модели документа (DOM) в рамках браузера.

7.6 Дети

Дети в онлайновой среде: как правило, родители контролируют общение своих детей в интернете, прослушивая или просматривая их действия, или же имеют информацию для ограничения доступа в удобном формате. Этот "защитный" метод может оказаться недоступным для родителей с ограниченными возможностями. Данная конкретная роль, в том виде, как она определена, лежит в двух областях: защита ребенка в онлайновой среде и доступность для взрослого лица/родителя с ограниченными возможностями, ответственного за воспитание детей с неограниченными, а также с ограниченными возможностями.

Дополнение I

Аспекты анализа когнитивной задачи в области кибербезопасности

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Аспекты анализа когнитивной задачи в области кибербезопасности

Анализ когнитивной задачи в целях кибербезопасности может включать в себя измерение элементов поведения, а также анализ взаимодействий, приводящих в конечном итоге к выводам в отношении внутренних мыслительных процессов. В настоящей Рекомендации рассматриваются три концепции информационной безопасности, а именно, конфиденциальность, целостность и доступность, а также требования к анализу когнитивной задачи в области кибербезопасности.

I.2 Три концепции, благоприятствующие информационной безопасности

Конфиденциальность

Измеряемые данные могут содержать личную информацию, которая чрезвычайно важна для неприкосновенности частной жизни. Следовательно, использование таких данных необходимо осуществлять с большой осторожностью и сопровождать заключением соглашений с конечными пользователями. Степень совместного использования такой информации должна находиться под жестким контролем.

Целостность

В этих методах измерений может использоваться собранная информация, независимо от боязни негативной оценки (FNE). Фактор FNE часто влияет на результаты наблюдений, из-за него некоторые люди будут скрывать свои человеческие ошибки, поскольку раскрытие ошибок часто наносит ущерб их собственной самооценке и профессиональному авторитету.

Доступность

Для наблюдений следует использовать метод, который легко применим к людям. В контексте предотвращения фишинга эти методы должны быть доступны во время просмотра пользователем представленной информации. Предпочтительными будут бесконтактные устройства. Кроме того, у пользователей не должно быть имплантатов или других устройств, которые могли бы каким-либо образом причинить им вред.

I.3 Возможные методы измерений

В исследованиях по экспериментальной психологии выявлена сильная связь между движением глаз и психическими расстройствами [b-Crawford, b-Noris]. Лей и др. [b-Leigh] классифицировали движения глаз по четырем категориям, а именно, быстрые скачкообразные движения глаз, фиксация, плавные следящие движения и вестибулярно-глазничные рефлексы. Как правило, характер скачкообразных движений глаз изменяется в зависимости от того, что человек видит. В контексте модели мышления, Ирвин и др. показали, что мысленное вращение подавляется во время этих движений глаз [b-Irwin], а Токуда [b-Tokuda] показал, что мыслительную нагрузку, являющуюся индикатором мыслительно/когнитивной занятости человека, можно оценивать по нарушениям в скачкообразных движениях глаз.

Проверка температуры кожи лица в качестве физиологической меры при оценке мыслительного состояния также является оправданным методом сбора информации [b-Or, b-Wang, b-Volskamp]. Согласно Генно и др. [b-Genno], их эксперименты показали, что когда субъекты испытывают такие чувства, как нервно-психическое напряжение и усталость, меняется температура в области носа. Кроме того, термография, в сочетании с другими методами измерений, представляет собой гибкое средство с высокой степенью автоматизации, позволяющее объективно оценивать рабочую нагрузку [b-Or].

Помимо этих решений для сбора информации часто используются измерения активности мозга, электрической проводимости кожи, параметров сердечной деятельности и артериального давления, однако для пользователей они довольно обременительны. Распознавание выражений лица и жестов полезно в отношении оценки доступности, однако они подвержены действию фактора FNE.

Дополнение II

Аспекты защиты конечного пользователя с учетом анализа когнитивной задачи

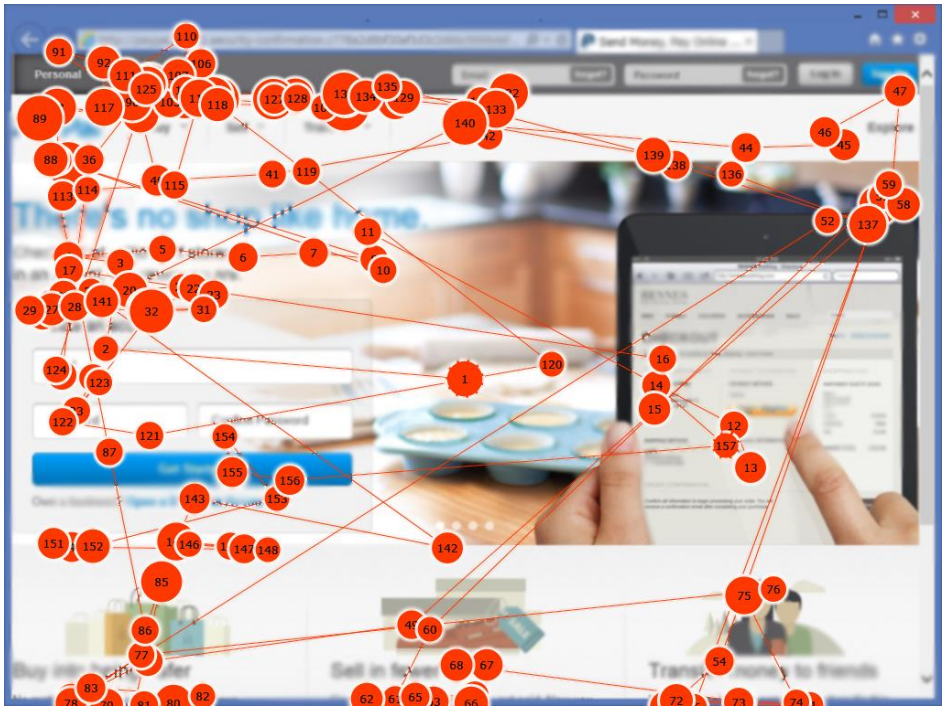
(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Оценка знаний и навыков пользователей

Проведенные в последнее время исследования показывают, что конечных пользователей можно разделить на две категории, а именно, на опытных и неопытных пользователей [b-Miyamoto]. Опытные пользователи, при вынесении суждения о степени доверия к сайту, оценивают в первую очередь URL сайта и/или показатель уровня защищенных сокетов (SSL), а не контент веб-страницы. Неопытные пользователи, напротив, судят, главным образом, по веб-контенту. Исходя из природы фишинга, веб-контент очень похож на контент легитимного сайта, что делает неопытных пользователей жертвами фишинговой ловушки.

Эти четко различия категорий конечных пользователей полезны для адаптации методов предотвращения фишинга под каждую из них. Возможным решением является обеспечение обнаружения фишинга с наименьшим ложноотрицательным результатом для неопытных пользователей, и наименьшим ложноположительным результатом для опытных пользователей. Как правило, в системах предотвращения фишинга существует проблема точности обнаружения, поскольку приходится выбирать компромиссные соотношения между ложноположительным (маркировка легитимных сайтов как фишинговых) и ложноотрицательными результатами (маркировка фишинговых сайтов как легитимных). Ложноположительные результаты будут увеличиваться, если эти системы будут концентрировать свое внимание на уменьшении ложноотрицательных результатов (маркировка фишинговых сайтов как легитимных). Снижение и тех и других ошибок считается трудной задачей. Несмотря на это, система должна защищать неопытных пользователей, которые часто ошибаются в принятии правильного решения.

Использование устройств для отслеживания движений глаз способствует идентификации неопытных пользователей среди пользователей веб. На рисунке II.1 представлены движения глаз неопытного пользователя, просматривающего фишинговый веб-сайт, а на рисунке II.2 – движения глаз опытного пользователя. Кружками отмечены точки фиксации зрения, а цифры внутри кружков обозначают последовательность фиксации. В случае для фишингового сайта, неопытный пользователь при оценке степени доверия просматривает содержание веб-сайта, но не обращает внимание на адресную строку браузера, как показано на рисунке II.1.

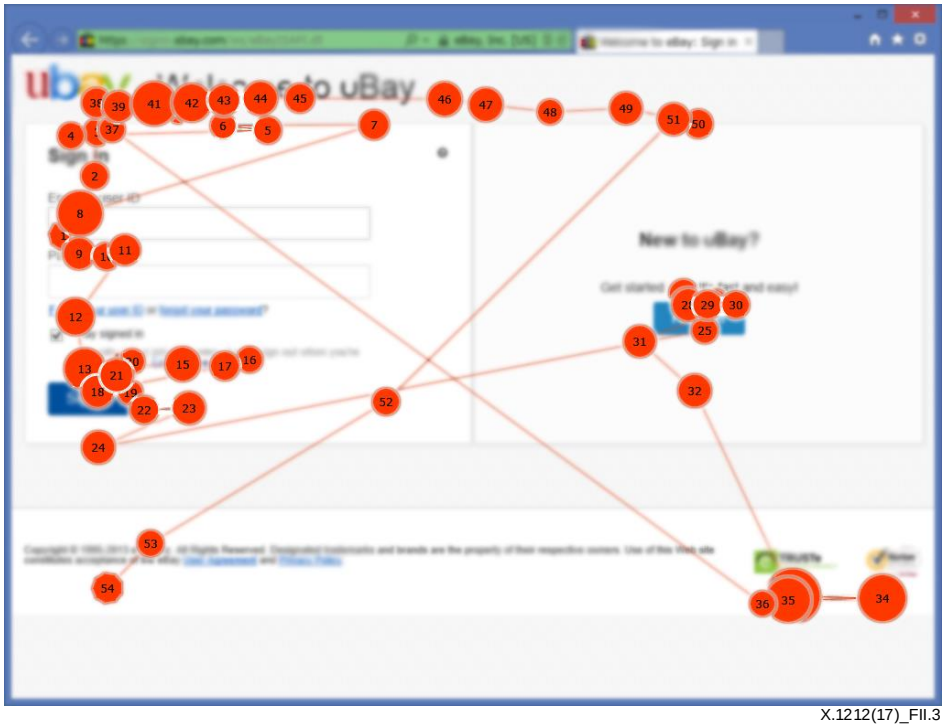


X.1212(17)_FII.1

Рисунок II.1 – Поведение неопытного пользователя на фишинговом веб-сайте

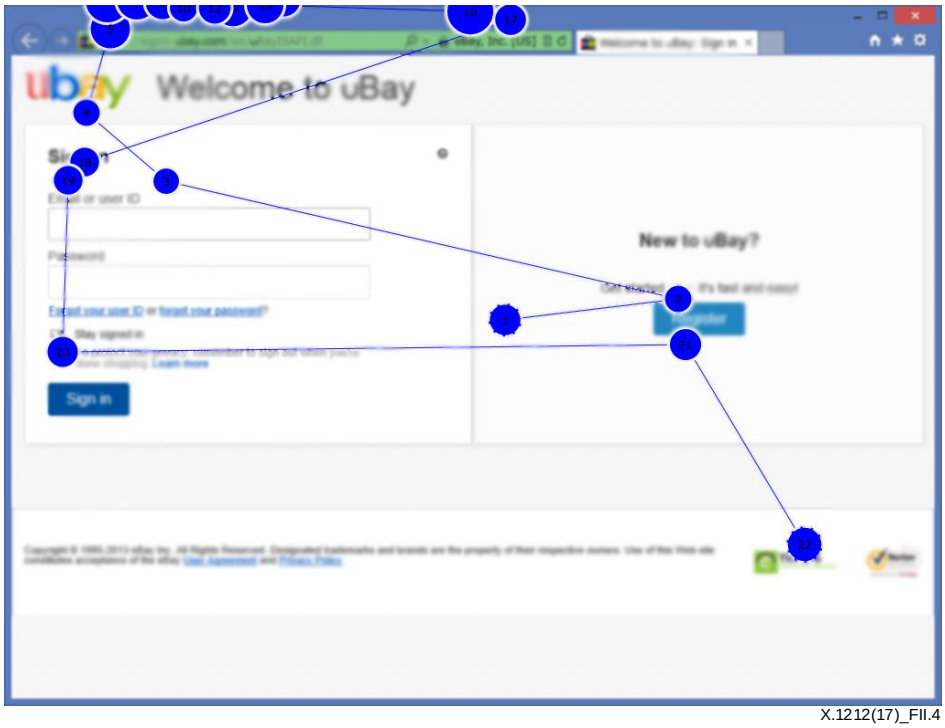
X.1212(17)_FII.2

Рисунок II.2 – Поведение опытного пользователя на фишинговом веб-сайте



X.1212(17)_FII.3

Рисунок II.3 – Поведение неопытного пользователя на легитимном веб-сайте



X.1212(17)_FII.4

Рисунок II.4 – Поведение опытного пользователя на легитимном веб-сайте

В случае легитимного сайта, пользователь обращает внимание только на контент веб-сайта, как показано на рисунке II.3. И наоборот, опытный пользователь при вынесении суждения о степени доверия обычно анализирует URL сайта и/или показатель SSL браузера, а не контент веб-страницы, как показано на рисунке II.4. Такие виды поведения при наблюдении показывают, что опытные пользователи обычно смотрят на адресную строку, на которой в начале просмотра отображаются URL и показатель SSL браузера. Неопытные пользователи не обращают на них внимание из-за нехватки знаний об URL или о показателях SSL.

Библиография

[b-ITU-T F.790] Рекомендация МСЭ-Т F.790 (2007 г.), *Руководящие принципы по доступности электросвязи для пожилых людей и людей с ограниченными возможностями.*
<https://www.itu.int/rec/T-REC-F.790>

[b-ITU-T F.791] Recommendation ITU-T F.791 (2015), *Accessibility terms and definitions*.
<https://www.itu.int/rec/T-REC-F.791>

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*
<https://www.itu.int/rec/T-REC-X.1252>

[b-ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта.*
<https://www.itu.int/rec/T-REC-X.1254>

[b-ITU-T X.1500] Рекомендация МСЭ-Т X.1500 (2011 г.), *Методы обмена информацией о кибербезопасности.*
<https://www.itu.int/rec/T-REC-X.1500>

[b-ITU-T-FSTP-TACL] МСЭ-Т FSTP-TACL (2006 г.), *Контрольный перечень по вопросам доступности электросвязи.*
<https://www.itu.int/publ/T-TUT-FSTP-2006-TACL>

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*.
<http://datatracker.ietf.org/doc/rfc5901/>

[b-IETF RFC 6376] IETF RFC 6376 (2011), *DomainKeys Identified Mail (DKIM) Signatures.*
<http://datatracker.ietf.org/doc/rfc6376/>

[b-ISO/IEC 40500] ISO/IEC 40500:2012, *Information Technology – W3C Web Content Accessibility Guidelines (WCAG) 2.0.*

[b-ANSI-Z535.4] ANSI (2011), Product Safety Signs and Labels.

[b-CAB-Baseline] CA/Browser Forum (2011), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* Version 1.0.
<http://www.cabforum.org/Baseline_Requirements_V1.pdf>

[b-Crawford] Crawford, T.J., Higham, S., Renvoize, T., Patel, J., Dale, M., Suriya, A., Tetley S. (2005), *Inhibitory control of saccadic eye movements and cognitive impairment in Alzheimer's disease*, Biological Psychiatry, vol. 9, no. 57.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report.*

[b-Felt2014] Felt, A.P., Reeder, R.W., Almuhimedi. H., Consolvo, S. (2014), *Experimenting At Scale With Google Chrome's SSL Warnings*, in Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems.

[b-Felt2015] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., Grimes, J. (2015), *Improving SSL Warnings: Comprehension and Adherence*, in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

[b-Genno] Genno, H., Ishikawa, K., Kanbara, O., Kikumoto, M., Fujiwara, Y., Suzuki, R., Osumi, M. (1997), *Using facial skin temperature to objectively evaluate sensations*, International Journal of Industrial Ergonomics, vol. 19.

[b-Irwin] Irwin, D.E., Brockmole, J.R. (2000), *Mental rotation is suppressed during saccadic eye movements*, Psychonomic Bulletin and Review, vol. 7, no. 4.

[b-Leigh] Leigh, R.J., Zee, D.S. (1991), *The Neurology of Eye Movements*, 4th ed. Oxford University Press.

[b-Miyamoto] Miyamoto, D., Iimura, T., Tazaki, H., Blanc, G., Kadobayashi, Y. (2014), *EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits*, in Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security.

[b-Noris] Noris, B. Benmachiche, K., Meynet, J., Thiran, J.P., Billard, A. (2007), *Analysis of Head-Mounted Wireless Camera Videos for Early Diagnosis of Autism*, Advances in Soft Computing, vol. 45.

[b-Or] Or, C.K.L., Duffy, V.G. (2007), *Development of a facial skin temperature-based methodology for nonintrusive mental workload measurement*, Occupational Ergonomics, vol. 7.

[b-Rigdon] Rigdon, M., Ishii, K., Watabe, M., and Kitayama, S. (2009), *Minimal social cues in the dictator game*, Journal of Economic Psychology vol. 30, iss. 3.

[b-Senju] Senju, A., Johnson, M.H. (2009), *The eye contact effect: mechanisms and development*, Trend in Cognitive Science.

[b-Tokuda] Tokuda, S., Obinata G., Palmer, E., Chaparro, A. (2011), *Estimation of mental workload using saccadic eye movements in a free-viewing task*, in Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society.

[b-UNCRPD] United Nations, Conventions on the Rights of Persons with Disabilities (2006).

[b-Volskamp] Voskamp, J., Urban, B. (2009), *Measuring Cognitive Workload in Non-military Scenarios Criteria for Sensor Technologies*, in Proceedings of the 5th International Conference on Foundations of Augmented Cognition.

[b-Wang] Wang, L., Duffy V.G., Du, Y. (2007), *A composite measure for the evaluation of mental workload*, in Proceedings of the 1st International Conference on Digital Human Modelling.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.