Auxiliary Material:

Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior

Yukiko Sawaya [*†] **Mahmood Sharif** [*‡] **Nicolas Christin** [‡] **Ayumu Kubota** [†]

Akihiro Nakarai [†] **Akira Yamada** [†]

NOTE

This document contains the Revised Security Behavior Intentions Scale (RSeBIS), knowledge in computer security, and self-confidence in computer-security knowledge questionnaires that we used in our paper [1]. The questionnaires are provided in Arabic, Chinese, English, French, Japanese, Korean, and Russian. If you use the knowledge or the self-confidence questionnaire, please cite our paper [1]. If you use RSeBIS in your work, please cite our paper as well as the original Security Behavior Intentions Scale (SeBIS) paper [1,2].

ARABIC

RSeBIS

1. أضبط هاتفي النقال ليقفل بشكل تلقائي بحال لم يتم إستعماله لفترة مطوّلة.
2. أستعمل كلمة مرور كي أفتح قفل حاسوبي.
3. أقفل حاسوبي عندما أبتعد عنه.
4. أستعمل كلمة مرور أو رقم سري كي أفتح قفل هاتفي النقال.
5. أغيّر كلمة مروري حتى عندما لا أحتاج لفعل ذلك.
6. أستعمل كلمة مرور مختلفة لحساباتي المختلفة.
7. عند فتح حساب جديد ,أحاول إختيار كلمة مرور أصعب من الحدّ الأدنى الذي يتطلبه الموقع.
8. أستعمل رموز وأحرف خاصّة في كلمة مرور حتى عندما لا يتطلّب مني الموقع ذالك.
9. عندما يبعث لي آخرون رابط ,أقوم بفتحه قبل أن أفحص لأي موقع سيتّخذني هذا الرابط.
10. أعرف الموقع الذي أزوره بعد أن أنظر على الرابط ,ليس فقط بحسب كيف تبدو لي الصفحة.
11. أتأكّد أنّ معلوماتي الخاصة ستبعث بشكل آمن (مثلا "https://", , SSL, او رمز قفل) قبل تسليمها إلى الموقع.
12. عند التصفّح ,أضع السهم فوق الروابط لأتأكّد أين سيتّخذونني.
13. إذا أكتشف مشكلة بأمن الحاسوب أحاول تصليحها أو أقوم بالإعلان عنها بدل أن أفترض أن أحد آخر سيقوم بذلك.
14. عندما يحثني جهاز أو برنامج معّين بتحديثه (update) أقوم بتحديثه بشكل فوري.
15. أتأكّد أنّ البرامج التي أستعملها قد تمّ تحديثها.
16. أتأكّد أنّ برامج الأنتيفايروس التي أستعملها تقوم بتحديث نفسها بشكل دائم.

Knowledge Questionnaire

1. ممكن تحديد الشركة التي تزودني بخدمات الإنترنت ومكاني من رقم ال-آي-بي (ip) الخاص بي.
2. ممكن تحديد رقم هاتفي من رقم ال-آي-بي (ip) الخاص بي.
3. معلومات عن متصفّح الإنترنت الذي أقوم بإستعماله ممكن تُكشف لأصحاب المواقع.
4. بما أنّ شبكات الواي-فاي (Wi-Fi) بالمقاهي تُأمّن على يد أصحاب المقاهي ,من الممكن أن أستعمل الشبكة لأبعث معلومات حساسة مثل رقم بطاقة الإئتمان الخاصة بي.
5. إنّه من الأصعب لقراصنة الحاسوب أن يخمّنوا كلمة مرور مكوّنة من كلمات عشوائية من أن يخمّنوا كلمات مرور مكوّنة من كلمات إستعمالها شائع.
6. إذا وصلتني رسالة بالبريد الإلكتروني تتطلّب مني تبديل كلمة مروري وتحوي رابط إلى الموقع ,فيجب أن أبدّل كلمة مروري بشكل فوري.
7. أجهزتي آمنة من أن تصاب ببرمجيّات خبيثة عندما أتصفح الإنترنت بما أن المتصفحات فقط يعرضون معلومات.
8. من المستحيل معرفة هل هناك إتصال آمن ما بين جهازي ومواقع الإنترنت.
9. من الممكن أن تُسرق معلوماتي إذا تظاهر موقع أفوم بزيارته بأنه موقع معروف (مثلا amazon.com).
10. من الممكن أن أعاني من خسارة مادّية إذا تظاهر موقع معّين أقوم بزيارته بأنّه موقع معروف.
11. أجهزتي وحساباتي قد تكون في خطر إذا أخطأت عند كتابة عنوان الموقع الذي أنوي زيارته.
12. عنوان ال-آي-بي (ip) الخاص بي هو سرّي ولا ينبغي أن أشارك به أي أحد.
13. إا لم يظهر متصفّح الإنترنت رمز قفل أخضر عندما أزور موقع معيّن, أستنتج أن هذا الموقع خبيث.
14. إنه من الآمن أن أفتح الروابط التي تصلني بالبريد الإلكتروني.
15. إنه من الآمن أن أفتح ملفّات تصلني بالبريد الإلكتروني.
16. أستعمل التصفّح الخاص (private browsing) كي لا تضرّ البرمجيّات الخبيثة جهازي.
17. إنه من الآمن أن أستعمل برنامج أنتيفتيروس قد تم تنزيله من خدمات الند لند (P2P) لإستبدال الملفّات.

---

[*]The first two authors contributed equally to this work.

[†]KDDI Research, Inc., Saitama, Japan.

{yu-sawaya, kubota, ak-nakarai, ai-yamada}@kddi-research.jp

[‡] Carnegie Mellon University, Pittsburgh, PA, USA.

{mahmoods, nicolasc}@cmu.edu

18. الأجهزه الإلكترونية آمنة إلّا إذا قام المستخدم بتحميل البرمجيّات الخبيثة بشكل فعّال.

Self-Confidence Questionnaire

1. أعرف وسائل لكي أمن المعلومات التي على أجهزتي من أن تُستغل.
2. أعرف وسائل لكي أتجنّب الخسارة المادية عند إستعمال الإنترنت.
3. أعرف وسائل لكي أمنع سرقة كلمات المرور الخاصة بي.
4. أعرف وسائل لكي أحافظ عى أجهزتي من أن تُخترق.
5. أعرف وسائل لكي أمتنع من أن يخدعني موقع زائف.
6. أعرف وسائل لكي أحمي المعلومات الخاصة بي من أن تُسرق عن تصفّح الإنترنت.

(SIMPLE) CHINESE

RSeBIS

1. 我为计算机设置了自动锁屏功能，长时间不用时计算机会自动锁屏。
2. 我为自己的笔记本和平板电脑设置了登陆密码。
3. 当我离开屏幕时我会手动为计算机锁屏。
4. 我为手机设置了锁屏密码。
5. 即便没有被强制定期更换密码，我也会不时主动更换密码。
6. 我为不同的账户设置不同的密码。
7. 当我创建一个在线账户时，我会使用长度超过该网站最低要求的密码。
8. 即便合法的密码可以不含特殊字符，我也会在密码中加入特殊字符。
9. 如果有人给我发送链接， 在不清楚该链接会把我带到哪去之前我不会点击它。
10. 我会通过地址栏上的 url 信息判断所访问网站的身份，而不是通过网站的内容与外观。
11. 在向网站提交信息之前我会先确认该信息是否能够安全传送(例如检查是否使用 SSL，"https://"，查看地址栏左侧锁型图标的状态)。
12. 在浏览网页时，我会先将鼠标放在一个链接上检查其 url 地址，确认之后再决定是否点击该链接。
13. 如果我发现了一个安全问题，我会修复该问题或向管理员汇报，而不是等着其他人去解决。
14. 每当被提醒有软件需要更新时，我会立刻更新。
15. 我会尽量保证自己所用的软件是最新版本。
16. 我会确保杀毒软件的自动更新功能正常运转。

Knowledge Questionnaire

1. 从我的 IP 地址可以知道我的网络服务商以及查到我的地理位置。
2. 从我的 IP 地址可以查到我的电话号码。
3. 网站管理者可以得知我的浏览器信息。
4. 咖啡店会确保其提供的 Wi-Fi 是安全的，所以我可以使用它传输敏感信息，比如信用卡账号等。
5. 比起常用的单词或表达作为密码，随机生成的密码更难被破解。
6. 当收到电子邮件要求我更换密码， 并给出了链接时，我应该立刻访问该链接并修改我的密码。
7. 因为浏览器只是展示网站信息的，所以浏览网页并不会导致我的计算机被病毒或木马感染。
8. 确认我的设备与网络服务器的通信是否使用了安全链接是无法做到的。
9. 如果我访问的是一个钓鱼网站(例如仿冒的购物网站或银行网站)，我的信息会被其窃取。
10. 访问钓鱼网站有可能导致经济上是损失。
11. 在输入网址时打错了，会给我的设备和账号带来一定的风险。
12. 我的 IP 地址属于敏感信息，与任何人分享 IP 地址都是不安全的。
13. 如果浏览器上没有出现一个绿色的锁型标志，那我正在访问一个恶意网站。
14. 打开收件箱中的电子邮件里的链接是安全的。
15. 打开电子邮件里的附件是安全的。
16. 使用隐私保护模式浏览网页可以保护我的设备不被病毒感染。
17. 使用 P2P 软件下载杀毒软件是安全的。
18. 只要用户不主动下载恶意软件，设备就不会被感染。

Self-Confidence Questionnaire

1. 我知道如何防止黑客入侵以保护自己设备上的数据。
2. 我知道如何防止在使用网络时可能造成的金钱损失。
3. 我知道如何防止我的 ID 和密码被盗。
4. 我知道如何防止我的设备被病毒或木马感染。
5. 我知道如何防止自己被钓鱼网站欺骗。
6. 我知道如何在浏览网站时防止数据被盗。

ENGLISH

RSeBIS

1. I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
2. I use a password/passcode to unlock my laptop or tablet.
3. I manually lock my computer screen when I step away from it.
4. I use a PIN or passcode to unlock my mobile phone.
5. I change my passwords even if it is not needed.
6. I use different passwords for different accounts that I have.
7. When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
8. I include special characters in my password even if it's not required.
9. When someone sends me a link, I open it only after verifying where it goes.
10. I know what website I'm visiting by looking at the URL bar, rather than by the website's look and feel.

11. I verify that information will be sent securely (e.g., SSL, "https://", a lock icon) before I submit it to websites.
12. When browsing websites, I mouseover links to see where they go, before clicking them.
13. If I discover a security problem, I fix or report it rather than assuming somebody else will.
14. When I'm prompted about a software update, I install it right away.
15. I try to make sure that the programs I use are up-to-date.
16. I verify that my anti-virus software has been regularly updating itself.

Knowledge Questionnaire

1. My Internet provider and location can be disclosed from my IP address.
2. My telephone number can be disclosed from my IP addresses.
3. The web browser information of my device can be disclosed to the operators of websites.
4. Since Wi-Fi networks in coffee shops are secured by the coffee shop owners, I can use them to send sensitive data such as credit card information.
5. Password comprised of random characters are harder for attackers to guess than passwords comprised of common words and phrases.
6. If I receive an email that tells me to change my password, and links me to the web page, I should change my password immediately.
7. My devices are safe from being infected while browsing the web because web browsers only display information.
8. It is impossible to confirm whether secure communication is being used between my device and a website.
9. My information can be stolen if a website that I visit masquerades as a famous website (e.g., amazon.com).
10. I may suffer from monetary loss if a website that I visit masquerades as a famous website.
11. My devices and accounts may be put at risk if I make a typing mistake while entering the address of a website.
12. My IP address is secret and it is unsafe to share it with anyone.
13. If my web browser does not show a green lock when I visit a website, then I can deduce that the website it is malicious.
14. It is safe to open links that appear in emails in my inbox.
15. It is safe to open attachments received via email.
16. I use private browsing mode to protect my machine from being infected.
17. It is safe to use anti-virus software downloaded through P2P file sharing services.
18. Machines are safe from infections unless users actively download malware.

Self-Confidence Questionnaire

1. I know about countermeasures for keeping the data on my device from being exploited.
2. I know about countermeasures to protect myself from monetary loss when using the Internet.
3. I know about countermeasures to prevent my IDs or Passwords being stolen.
4. I know about countermeasures to prevent my devices from being compromised.
5. I know about countermeasures to protect me from being deceived by fake web sites.
6. I know about countermeasures to prevent my data from being stolen during web browsing.

FRENCH

RSeBIS

1. Je paramètre mon ordinateur de façon à ce que l'écran se vérouille automatiquement quand je ne l'utilise pas pendant un certain temps.
2. J'utilise un mot de passe ou un code PIN pour déverouiller mon ordinateur portable ou ma tablette.
3. Je vérouille manuellement mon écran d'ordinateur quand je m'en éloigne.
4. J'utilise un code pour déverouiller mon téléphone portable.
5. Je change mes mots de passe même quand ce n'est pas nécessaire.
6. J'utilise des mots de passe differents pour les différent comptes que je possède.
7. Quand je crée un nouveau compte en ligne, j'essaye d'utiliser un mot de passe qui va au-delà des exigences de sûreté du site.
8. J'utilise des caractères spéciaux dans mon mot de passe même si cela n'est pas requis.
9. Quand quelqu'un m'envoie un lien, je l'ouvre seulement après avoir confirmé où il m'emmène.
10. Je sais quel est le site Web que je visite en me fiant à la barre d'adresse, plutôt qu'à l'apparence visuelle du site.
11. Je confirme que mes informations sont envoyées de façon sûre (par example, SSL, “https://”, icône de cadenas) avant de les envoyer à des sites Web.
12. Quand je navigue sur un site Web, je fais passer ma souris sur les liens pour voir où ils m'emmènent, avant de cliquer dessus.
13. Si je découvre une faille de sécurité, je la colmate ou la signale plutôt que de supposer que quelqu'un d'autre le fera.
14. Quand je suis invité à mettre à jour un logiciel, je fais cette mise-à-jour immédiatement.
15. J'essaye de faire en sorte que les logiciels que j'utilise soient à jour.

16. Je vérifie que mon anti-virus est régulièrement mis à jour automatiquement.

Knowledge Questionnaire

1. Mon fournisseur d'accès Internet et ma localisation peuvent être révélés par mon adresse IP.
2. Mon numéro de téléphone peut être révélé par mon adresse IP.
3. Les informations sur le navigateur Web de ma machine peuvent être révélées aux opérateurs de sites Web.
4. Étant donné que les réseaux wi-fi dans les cafés sont sécurisés par les propriétaires de ces cafés, je peux me servir de ces réseaux pour envoyer des données sensibles comme des numéros de carte de crédit.
5. Les mots de passe qui consistent de caractères pris au hasard sont plus durs à deviner que les mots de passe qui consistent de mots ou de phrases communes.
6. Si je reçois un e-mail qui me dit de changer mon mot de passe, et a un lien vers une page web, je me dois de changer mon mot de passe immédiatement.
7. Mes machines sont à l'abri des infections lorsque je navigue le Web, parce que le navigateur se contente de présenter des informations.
8. Il est impossible de confirmer qu'une communication sécurisée est utilisée entre ma machine et un site web.
9. Mes informations personelles peuvent être volées si un site Web que je visite imite un site Web connu (par exemple, amazon.com).
10. Je peux encourir des pertes d'argent si un site Web que je visite imite un site Web connu.
11. Mes machines et comptes en ligne peuvent encourir des risques si je fais un erreur de frappe en tapant l'adresse d'un site Web.
12. Mon adresse IP est un secret, et il est dangereux de la partager avec qui que ce soit.
13. Si mon navigateur Web ne montre pas un cadenas vert quand je visite un site Web, je peux en déduire que le site Web est malveillant.
14. Ouvrir des liens qui apparaissent dans des e-mails dans ma boîte aux lettres est sûr.
15. Ouvrir des pièces jointes reçues par e-mail est sûr.
16. Je me sers du mode de navigation privée pour protéger ma machine contre les infections.
17. Utiliser un anti-virus téléchargé sur un réseau pair-à-pair de partage de fichiers est sûr.
18. Les machines sont à l'abri des infections, à moins que les utilisateurs ne téléchargent activement des logiciels malveillants.

Self-Confidence Questionnaire

1. Je connais les contre-mesures pour éviter que les données de ma machine ne soient exploitées à des fins malveillantes.
2. Je connais les contre-mesures pour me protéger contre les pertes d'argent quand je me sers d'Internet.
3. Je connais les contre-mesures pour éviter que mes informations privées ou mes mots de passe ne soient volés.
4. Je connais les contre-mesures pour éviter que mes machines ne soient compromises.
5. Je connais les contre-mesures pour éviter d'être trompé par des sites Web contrefaits.
6. Je connais les contre-mesures pour éviter que mes données ne soient volées lorsque je navigue sur le Web.

JAPANESE
RSeBIS

1. 長時間パソコンを使用しない場合、自動的に画面がロックされるように設定している。
2. ノートパソコンやタブレットにパスワードロックをかけている。
3. パソコンから離れる際は、手動でパソコンの画面をロックしている。
4. 携帯電話やスマートフォンのロックを解除する際はパスワード（パターンロック、指紋認証なども含む）を入力する。
5. 必要に迫られなくとも、パスワードを定期的に変えている。
6. アカウントや ID 毎に異なるパスワードを設定している。
7. インターネットサービスのアカウント作成、及びにパスワード設定をする際は、ウェブサイトが要求する条件よりも安全性の高いパスワードを設定している。
8. 特別要求されなくても、自分のパスワードに特殊な文字を含めている。
9. 誰かからウェブサイトへのリンクが送られてきた際は、実際にどこにつながるかを確認した後でリンクを開く。
10. ウェブサイトの見た目と印象ではなく、ウェブ閲覧ソフトの URL 欄を見て、どのページに接続しているかを判断する。
11. 安全に情報が送られるか(“https://""や錠マーク) をあらかじめ検証した後で、ウェブサイトで情報を入力し送信する。
12. ウェブサイトを閲覧する際、リンクにマウスを重ね、実際にどのサイトへ移動するか確認する。
13. インターネットを利用している最中にセキュリティ上の問題を見つけた場合には、自分自身で解決したり、誰かに解決を依頼したりするなど解決策を模索する。
14. ソフトウェアの更新を促されたら、すぐに更新をする。
15. 利用しているソフトウェアが最新版であることを確認しようとする。

16. ウィルス対策ソフトが定期的に自動更新する設定になっているかどうかを確認する。

Knowledge Questionnaire

1. IP アドレスから、利用しているプロバイダや地域が第三者に知られることがある。
2. IP アドレスから、電話番号が第三者に知られることがある。
3. 使用しているウェブ閲覧ソフト情報などはウェブサイト管理者に知られることがある。
4. 喫茶店等の Wi-Fi は店のオーナーがセキュリティ対策をしているので、クレジットカード番号のようなプライバシ情報を入力してもよい。
5. 単語や意味のあるフレーズを含むパスワードよりもランダムな文字列のパスワードの方が攻撃者は推測しづらい。
6. パスワードの変更を指示する旨とウェブページへのリンクがメールで届いた際は、すぐにリンク先にアクセスし、パスワードを変更する必要がある。
7. ウェブ閲覧ソフトは情報を表示するだけなので、ウェブ閲覧ソフトを通じてウィルスに感染することはなく安全である。
8. 利用している PC・スマートフォン・タブレットと Web サイトの間が安全な通信になっているかを確認することは難しい。
9. 有名なサイトに偽装したウェブサイトにアクセスしてしまった場合、自分の個人情報が詐取されることがある。
10. 有名なサイトに偽装したウェブサイトにアクセスしてしまった場合、金銭的被害が生じることがある。
11. URL の打ち間違いをした場合、デバイスやアカウントが危険にさらされるかもしれない。
12. 自分の IP アドレスは秘密情報であり、他人に伝えることは危険である。
13. 緑の南京錠マークがついていないウェブサイトを閲覧しているときは、悪意のあるサイトと思った方がいい。
14. 受信メール内に記載のウェブサイトへのリンクは安全だ。
15. メールで受信した添付ファイルを開くのは安全だ。
16. PC・スマートフォン・タブレットのウィルス感染を防ぐために、プライベートブラウジングモードを使うと安全である。
17. P2P ファイル共有サービス経由でダウンロードしたウィルス対策ソフトを利用するのは安全である。
18. ウィルスを能動的にダウンロードしない限りウィルス感染を防ぐことができる。

Self-Confidence Questionnaire

1. パソコン・スマホ・タブレットのデータが悪用されないようにするための対策手段を知っている。
2. インターネット利用時に金銭被害を受けないための対策手段を知っている。
3. ID やパスワードが盗まれないようにするための対策手段を知っている。
4. パソコン・スマホ・タブレットが不正に侵入されるのを防ぐための対策手段を知っている。
5. 偽物の Web サイトに騙されるのを防ぐ対策手段を知っている。
6. ウェブ閲覧時に自分の情報が詐取されるのを防ぐための対策手段を知っている。

KOREAN

RSeBIS

1. 오랫동안 사용하지 않으면 컴퓨터 화면이 자동으로 잠기도록 설정합니다.
2. 노트북이나 태블릿의 잠금을 해제하기 위한 비밀번호/암호를 사용합니다.
3. 다른 곳으로 이동할 때는 수동으로 컴퓨터 화면을 잠급니다.
4. 휴대 전화의 잠금을 해제하기 위한 PIN 이나 암호를 사용합니다.
5. 특별히 필요하지 않은 경우에도 가끔 비밀번호를 변경합니다.
6. 가지고 있는 서로 다른 계정에 대해 각각 다른 비밀번호를 사용합니다.
7. 새로운 온라인 계정을 만들 때, 해당 사이트의 최소 요구사항보다 더 강력한 비밀번호를 사용하려고 노력합니다.
8. 필수 조건이 아니어도 비밀번호에 특수 문자를 포함합니다.
9. 누군가 나에게 링크를 보낼 경우, 그 링크가 어느 사이트로 향하는지 확인한 후에 엽니다.
10. 웹 사이트의 모양과 느낌이 아닌 URL 표시줄을 보고 방문한 웹 사이트를 판단합니다.

11. 웹 사이트에서 입력 내용을 제출하기 전에 (예를 들어, SSL, "https://", 잠금 아이콘 등을 보고) 내 정보가 안전하게 전송되는가를 확인합니다.
12. 웹 사이트를 검색할 때 링크에 마우스 포인트를 올려서 어디로 향하는지 확인한 후에 클릭합니다.
13. 보안과 관련된 문제를 발견하면, 다른 사람이 처리하겠지 하고 생각하기보다 내가 직접 문제를 수정하거나 보고합니다.
14. 소프트웨어 업데이트를 묻는 메시지를 보면 곧바로 업데이트를 설치합니다.
15. 사용하는 프로그램이 최신 버전인지 확인하려고 노력합니다.
16. 사용 중인 안티바이러스 소프트웨어가 정기적으로 자체 업데이트를 하고 있는지 확인합니다.

Knowledge Questionnaire

1. IP 주소를 통해 이용 중인 인터넷 공급자와 위치를 알아낼 수 있습니다.
2. IP 주소를 통해 전화번호를 알아낼 수 있습니다.
3. 웹 사이트의 운영자가 내가 사용하는 단말의 웹 브라우저 정보를 알아낼 수 있습니다.
4. 커피숍의 Wi-Fi 무선 네트워크는 커피숍 소유주가 보안을 철저히 하고 있으므로, 신용카드 정보와 같은 민감한 데이터를 전송하는 데 사용할 수 있다고 생각합니다.
5. 임의의 문자로 구성된 비밀번호는 해커가 추측하기에 일반적인 단어와 구문으로 구성된 비밀번호보다 더 어렵습니다.
6. 비밀번호를 변경하도록 안내하는 메시지와 함께 웹 페이지로 연결되는 링크가 포함된 이메일을 받았을 때는 즉시 비밀번호를 변경해야 합니다.
7. 웹 브라우저는 단순히 정보를 표시하기만 할 뿐이므로, 웹을 검색하는 동안에는 내 컴퓨터가 감염될 위험은 없습니다.
8. 내 컴퓨터와 웹 사이트 사이에 보안 통신이 이용되고 있는지는 확인할 수 없습니다.
9. (amazon.com 과 같은) 유명한 웹 사이트로 위장한 가짜 웹 사이트를 방문할 경우 내 정보가 도난당할 수 있습니다.
10. 유명한 웹 사이트로 위장한 가짜 웹 사이트를 방문할 경우, 금전적인 손해를 입을 수 있습니다.
11. 웹 사이트의 주소를 입력하는 동안에 입력 실수를 하면 내 컴퓨터와 계정이 위험해질 수 있습니다.
12. 내 IP 주소는 비밀이며 다른 사람과 공유하는 것은 안전하지 않습니다.
13. 웹 사이트를 방문할 때 웹 브라우저에서 녹색 잠금 표시가 나타나지 않을 경우, 해당 웹 사이트는 보안이 취약한 사이트라고 추측할 수 있습니다.
14. 받은 편지함에 있는 이메일에 포함된 링크를 여는 것은 안전합니다.
15. 이메일로 받은 첨부 파일을 여는 것은 안전합니다.
16. 컴퓨터 바이러스의 감염으로부터 컴퓨터를 보호하기 위해 웹 브라우저를 개인 정보 보호 모드에서 사용합니다.
17. P2P 파일 공유 서비스를 통해 내려받은 안티바이러스 소프트웨어를 사용하는 것이 안전합니다.
18. 사용자가 일부러 악성 코드를 내려받지 않는 한 컴퓨터는 바이러스의 감염으로부터 안전합니다.

Self-Confidence Questionnaire

1. 나는 내 컴퓨터의 데이터를 보안 침해 사고로부터 보호하기 위한 대책에 대해 알고 있습니다
2. 나는 인터넷을 사용할 때 금전적 손실로부터 자신을 보호하기 위한 대책에 대해 알고 있습니다
3. 나는 내 ID 또는 비밀번호가 도난당하지 않도록 하는 대책에 대해 알고 있습니다
4. 나는 내 컴퓨터를 (컴퓨터 바이러스 감염 등의) 손상으로부터 보호하기 위한 대책에 대해 알고 있습니다
5. 나는 가짜 웹 사이트에 속지 않는 방법에 대해 알고 있습니다

6. 나는 웹 검색하는 동안 내 데이터가 도난되지 않도록 보호하기 위한 대책에 대해 알고 있습니다

RUSSIAN

RSeBIS

1. Я настраиваю экран компьютера на автоматическую блокировку, когда долго его не использую.
2. Я использую пароль для разблокировки компьютера.
3. Я вручную блокирую экран компьютера, когда от него отхожу.
4. Я использую PIN или пароль для разблокировки мобильного телефона.
5. Я меняю пароль, даже когда в этом нет необходимости.
6. Я использую разные пароли для разных аккаунтов.
7. При создании новых онлайн-аккаунтов я использую пароли которые превышают минимальные требования.
8. Я использую в паролях специальные символы даже при отсутствии этого требования.
9. Когда мне присылают ссылку, я открываю ее только после того, как проверяю куда она ведет.
10. Я знаю который веб-сайт я посещаю по URL-адресу, а не по виду и содержимому веб-сайта.
11. Перед загрузкой информации на веб-сайт я убеждаюсь в безопасной отправке (SSL, "https://", знак замка и т.д.).
12. Перед открытием ссылки я всегда проверяю, куда она ведет, наведя на нее курсор.
13. При возникновении проблем с безопасностью я ни на кого не полагаюсь ,и самостоятельно их исправляю или сообщаю о них.
14. Получив сообщение о доступном обновлении програмы, я тут же устанавливаю его.
15. Я всегда обновляю программы, которыми я пользуюсь.
16. Я слежу за тем, чтобы моя антивирусная программа регулярно обновлялась.

Knowledge Questionnaire

1. Мой IP-адрес позволяет определить Интернет-провайдера и местоположение.
2. Мой IP-адрес позволяет определить номер телефона.
3. Владельцы веб-сайтов могут получать доступ к информации про браузер которым я пользуюс.
4. Сети Wi-Fi в кофейнях защищены их владельцами, поэтому я могу отправлять через них конфиденциальную информацию (например, данные кредитной карточки).
5. Злоумышленникам труднее угадать пароль, представляющий собой случайную комбинацию символов, чем пароль, состоящий из общеупотребительных слов или фраз.
6. Получив электронное сообщение что надо менять пароль, со ссылкой на сайт, я немедленно меняю пароль.
7. Устройство не может заразиться через веб-браузер, так как он просто отображает информацию.
8. Я не могу определить, используется ли безопасная связь между моим устройством и веб-сайтом.
9. Мою информацию можно украсть, если веб-сайт маскируется под известный веб-сайт (например, amazon.com).
10. Я могу понести финансовый ущерб, если веб-сайт, на который я захожу, маскируется под известный веб-сайт.
11. Мои устройства и аккаунты могут подвергнуться риску, если я допущу ошибку при вводе адреса веб-страницы.
12. Мой IP-адрес – это секретная информация, и никто не должен его узнать.
13. Если при посещении веб-сайта в браузере нет значка с зеленым замком, этот веб-сайт небезопасен.
14. Мне безопасно переходить по ссылкам, которые мне присылают по электронной почте.
15. Мне безопасно открывать вложения, полученные по электронной почте.
16. Я использую режим приватного просмотра, чтобы защитить устройство от вирусов.
17. Я могу без опаски использовать антивирус, загруженный с файлообменника.
18. Устройство не может быть заражено, если активно не скачивать вредоносные программы.

Self-Confidence Questionnaire

1. Я знаю, как защитить данные на устройстве от использования третьими сторонами.
2. Я знаю, как защитить себя от финансовых рисков при использовании Интернета.
3. Я знаю, как защитить ID и пароли от злоумышленников.
4. Я знаю, как защитить мои устройства.
5. Я знаю, как защитить себя от ложных веб-сайтов.
6. Я знаю, как защитить свои данные от злоумышленников при использовании Интернета.

REFERENCES

[1] Yukiku Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akhiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proc. CHI.*

[2] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proc. CHI.*