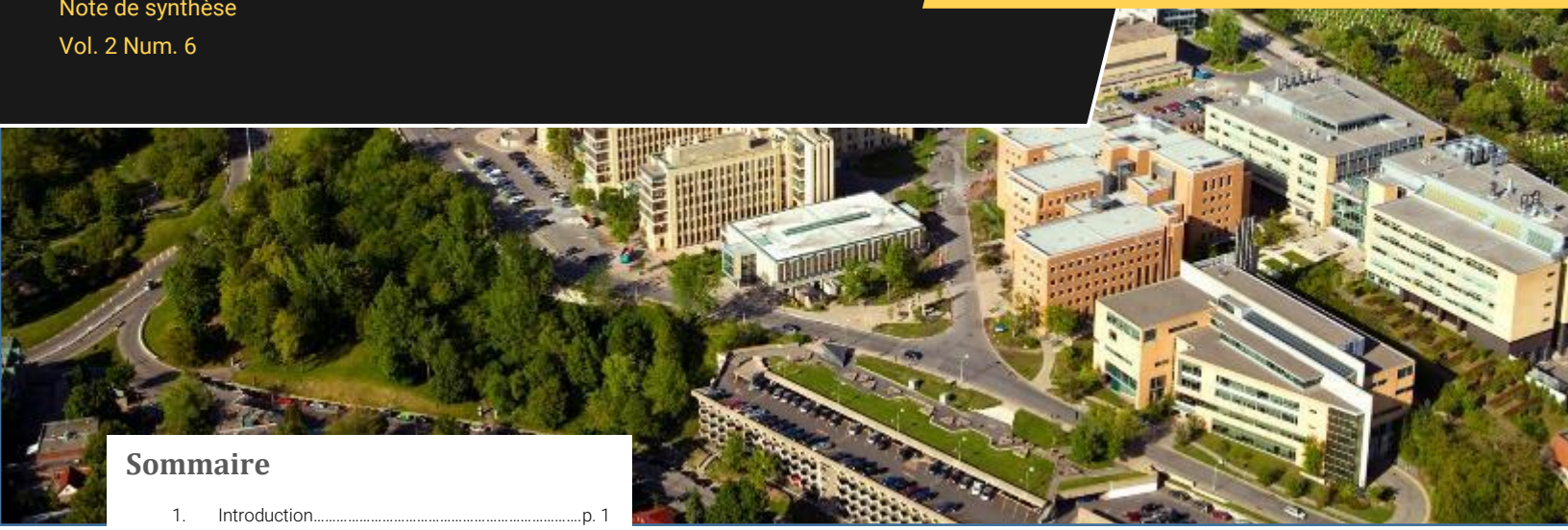
Les perceptions de risques et de sécurité

Lorédane Piris, candidate à la maîtrise

Note de synthèse
Vol. 2 Num. 6

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

L'étude des perceptions qu'ont les utilisateurs de la sécurité et des risques auxquels ils font face relève de différents champs de recherche comme la santé publique, la psychologie et la criminologie. Ce dernier domaine de recherche est particulièrement utile pour analyser les mécanismes de prévention de la cybercriminalité, car il nous permet de comprendre comment les individus prennent des décisions et adoptent (ou pas) des comportements de protection lorsqu'ils se retrouvent dans des contextes d'incertitude ou d'imprévisibilité. Il nous permet également de comprendre l'acceptabilité ou le refus d'une mesure de sécurité. Ainsi, si l'on souhaite améliorer la cybersécurité des utilisateurs, nous devons porter notre attention sur les diverses manières dont les utilisateurs perçoivent les risques et y répondent[1, 2].

Perceptions et risques

Définitions

Une perception est définie comme un « **événement cognitif dans lequel un stimulus ou un objet, présent dans l'environnement immédiat d'un individu, lui est représenté dans son activité psychologique interne en principe de façon consciente**. »[3]

La **perception du risque** quant à elle répond à plusieurs définitions selon les orientations théoriques, mais il s'agit généralement de « **l'évaluation subjective par une personne de la probabilité qu'un événement spécifique se produise et de la façon dont elle se sent concernée par ses conséquences** ».[4]

Les facteurs de variance des perceptions

Une difficulté de la circonscription de la perception du risque est que cette dernière se modifie au contact des usagers et les risques n'ont pas la même signification pour tous. Non seulement, lorsqu'une personne se familiarise avec certains risques, les perceptions qu'elle en a peuvent être amenées à se modifier une fois identifiés comme tels, mais une multitude de facteurs entrent également en jeu et peuvent évoluer selon le contexte. [1, 5, 6]

Différences de perceptions selon le profil de l'utilisateur

Les perceptions de la sécurité et des risques varient en fonction de **l'âge, du sexe, du niveau d'éducation, du statut professionnel, du statut socio-économique, du niveau d'expérience en informatique, de l'attitude, mais aussi au gré des facteurs psychologiques, sociaux ou culturels**. Différentes études s'attardent généralement sur l'une ou l'autre de ces variables, mais ne les abordent pas toutes ensemble. Souvent, l'accent est mis sur les différences entre les utilisateurs ordinaires et les experts, car celles-ci sont telles qu'elles précipitent généralement des problèmes communicationnels entre ces deux groupes (par exemple, pour offrir ou recevoir des conseils de sécurité). [1, 4, 6, 7, 8]

Différences de perceptions selon le risque et sa cible

Lorsqu'il s'agit d'évaluer un risque, les gens ne feront pas les mêmes calculs de probabilité selon que ceux-ci se matérialisent et les touchent directement ou bien affectent potentiellement les autres. Généralement, les gens se sentent moins concernés par les risques pour eux-mêmes.[9]

Le rôle du sentiment de contrôle et le caractère volontaire du risque

Lorsqu'un risque est perçu comme volontaire et sous contrôle, il apparaît alors comme **moins probable et sévère pour la personne**, ce qui va avoir pour conséquences une sous-estimation et par conséquent une diminution des comportements de protection. [1, 8, 9]

Sensibilité aux risques et inquiétudes

Certains individus peuvent être très sensibles aux risques et ainsi s'inquiéter facilement de tous les dangers, tandis que d'autres restent imperturbables. Cependant, **certains risques peuvent représenter plus de préoccupations que d'autres**. Par exemple, les utilisateurs d'internet expriment être plus inquiets face aux menaces contre l'information que pour les menaces à l'encontre des personnes ou de la technologie. Certaines conséquences sont aussi plus inquiétantes que d'autres pour un même danger. Par exemple, lors d'un vol de données compromettant des informations personnelles (par exemple, nom, date de naissance, adresse, etc.), généralement c'est le vol du numéro de sécurité sociale qui va préoccuper le plus les individus.[4, 9, 10]

Risques perçus et menaces

Les risques perçus ne sont pas les mêmes selon la menace, et **les utilisateurs ne semblent pas avoir les mêmes perceptions sur ce qui semble le plus dangereux**. En outre, si on peut retrouver plusieurs niveaux de risque et de menaces selon les activités en ligne, **certaines menaces vont augmenter les niveaux de perceptions de risques et de vulnérabilité des utilisateurs** (par exemple, menace qui compromet l'intégrité de l'information). Enfin, les utilisateurs peuvent être conscients des multiples menaces, mais peuvent choisir, par souci de simplification, de **focaliser leurs mesures de**

protection seulement sur l'élément qu'ils comprennent ou maîtrisent le mieux (par exemple, seulement sur les mots de passe). Ils vont ainsi prioriser certains risques au détriment d'autres qui sont pourtant plus probables statistiquement ou plus sévères. [1, 4, 5, 11]

Augmentation du risque perçu

Le potentiel catastrophique va augmenter le niveau de risque perçu surtout si celui-ci produit un fort impact ou bien s'il a des conséquences graves. Les risques rares vont provoquer de la terreur à l'inverse des risques courants, alors que ces derniers provoquent des préjudices plus importants du fait de leur fréquence.[1, 6]

Perceptions et émotions

Les gens vont percevoir et évaluer les risques en fonction de ce qui est pensé, faisant appel à des processus rationnels et analytiques, mais aussi selon leur ressenti, les émotions étant impliquées dans la perception, la gestion et l'acceptation du risque. Les humeurs et affects constituent une toile de fond sur laquelle les perceptions et pensées concernant les risques fluctuent. Par exemple, une personne de bonne humeur percevra moins les risques qui l'entourent, et lors d'une activité, la personne éprouvant des sentiments positifs jugera les risques comme moins probables de se manifester et accentuera les avantages liés aux comportements risqués.[12, 13, 14]

En outre, ***l'heuristique d'affect*** modifie également nos perceptions. Il s'agit d'un raccourci cognitif qui altère le jugement et permet une prise de décision rapide en simplifiant les opérations psychiques de l'individu à partir des émotions. Ainsi, les technologies perçues comme plus avantageuses seront perçues comme moins risquées et inversement.[1, 14]

Enfin, les émotions fortes modifient elles aussi les estimations des risques, puisque par exemple la peur va les intensifier alors que la colère va les minimiser. De plus, la perception du risque sera aussi modifiée si ces émotions se lient à des facteurs comme la gravité perçue, l'immédiateté ou bien si l'utilisateur se sent affecté personnellement. Par exemple, la perception du risque, la crainte et l'évaluation de la gravité sont plus élevées pour les vols d'identité que pour la fraude amoureuse (une pratique frauduleuse dans laquelle un arnaqueur va attirer des étrangers dans des relations intimes sur les réseaux sociaux, sous une fausse identité pour leur soutirer de l'argent).[1, 14]

Perceptions et variations : L'être humain, ses connaissances et ses calculs

Les éléments inhérents à la nature humaine

Les modèles mentaux, les biais et la confiance vont agir comme des mécanismes de simplification de la complexité. Ils sont non seulement utiles pour appréhender les différentes perceptions, mais aussi importants à considérer, car en les comprenant et en les intégrant dans nos approches, il est possible d'adapter les stratégies de communication et les interfaces technologiques afin d'aider et d'encourager les utilisateurs à avoir des comportements vertueux.

Les modèles mentaux

« Les modèles mentaux sont les représentations de la façon dont les objets ou les systèmes fonctionnent dans l'esprit des gens », de la manière dont ils conçoivent des situations imaginaires, hypothétiques ou réelles, ou encore des problèmes récurrents[4]. Ces représentations nous permettent de comprendre la perception de la sécurité et des risques, en mettant en évidence le raisonnement individuel, la prise de décision et la compréhension des menaces et leurs conséquences probables. En cybersécurité, les utilisateurs mobilisent souvent des modèles mentaux inexacts ou fragmentés des menaces, des risques, mais aussi des conséquences de leurs actions face à la sécurité.[4, 11, 15]

Les biais

Un biais cognitif est un mécanisme interne qui s'écarte de la pensée rationnelle ou logique, qui va

altérer le jugement et donner lieu à une prise de décision faussée. Plusieurs biais cognitifs peuvent influencer les perceptions, tels que le biais de supériorité, d'optimisme, d'invulnérabilité, ou encore l'illusion de contrôle. Interreliés, ils peuvent mettre les gens dans des situations de prise de risque, car ces « illusions positives »[2] vont donner la sensation aux gens qu'ils ne seront pas aussi vulnérables ou exposés aux conséquences négatives que leurs pairs. Ils vont ainsi sous-estimer les dangers, ce qui va influencer leur prise de décision. Par exemple dans le cas d'un vol des données, l'individu va penser que seuls les individus plus aisés financièrement sont ciblés. [2, 4, 5, 11]

La confiance

La confiance en soi peut-être à **double tranchant**. On observe, qu'elle peut permettre aux gens de se comporter de manière plus sûre et de se protéger lorsqu'il s'agit de contrôler les dangers qu'ils perçoivent, d'autant plus s'ils croient fortement en leur capacité à accomplir la tâche (on peut également parler d'auto-efficacité)[11, 16, 17]. Cependant, avoir trop confiance en soi peut avoir l'effet inverse, car cela peut biaiser les perceptions de la sécurité. L'individu qui a trop confiance en lui-même se pensera suffisamment protégé, réduira sa vigilance et ne percevra plus les risques adéquatement (par exemple, des experts vont cliquer sur des pièces jointes provenant d'un courriel envoyé par un inconnu).[18]

L'expérience

L'expérience passée des utilisateurs, mais aussi celles des autres influence la perception de la sécurité et des risques de plusieurs manières.

Tout d'abord, les expériences de prise de risque, si elles n'ont pas engendré de conséquences négatives pour la personne, l'amèneront à **sous-estimer les risques pour sa sécurité**.

Deuxièmement, **une expérience négative passée avec la technologie**, touchant ou non à la sécurité, donnera naissance à **une perception négative qui aura des conséquences sur ses choix futurs**, y compris sur la sécurité. Par exemple, des mises à jour de sécurité peuvent être refusées par les utilisateurs en raison d'une mauvaise expérience antérieure avec des mises à jour du système d'exploitation.

Troisièmement, les utilisateurs se réfèrent aux expériences des autres (p. ex., blogues, avis sur internet, histoires informelles), car cela offre des **exemples réels de situation positive ou négative** à laquelle ils peuvent s'identifier.[4, 6, 15, 19, 20]

L'impact des connaissances, de l'accès aux informations et de la compréhension

Connaissances et compréhension de la sécurité, des risques et menaces

Les connaissances, la compréhension et l'accès aux informations participent aux perceptions de la sécurité et des risques, et de ce fait, à la prise de décision et au comportement de sécurité. D'abord, parce que **la connaissance est importante pour aider à combler l'écart entre la sécurité réelle et la sécurité perçue** des gens, notamment parce que ce que les gens pensent savoir va affecter leur comportement en matière de sécurité de façon plus marquée que ce qu'ils ne savent vraiment. Ainsi, s'ils pensent comprendre les risques, leurs perceptions de ceux-ci s'en trouvent diminuée.[16, 21]

De plus, concernant la compréhension des menaces, les utilisateurs ont parfois de la difficulté à déterminer ce qui les concerne directement ou ce qui affecte leur sécurité et leurs comportements de protections. **Sans compréhension fiable des menaces, de leurs conséquences, mais aussi des conseils offerts, les utilisateurs choisiront de les ignorer**. Enfin, même si un risque est perçu comme élevé, le manque de connaissances peut plonger la personne dans la paralysie et l'inaction alors qu'elle devrait normalement se protéger.[4, 22, 23]

Débat sur les connaissances

Le manque de connaissances des utilisateurs sur les pratiques sécuritaires et les risques fait l'objet de nombreux débats. Certaines études affirment que les utilisateurs comprennent bien les risques, mais qu'ils fonctionnent en réalité stratégiquement

afin de réduire le fardeau que représente l'application des conseils de sécurité (par exemple, réutiliser des mots de passe pour plusieurs comptes).[24, 25]

Ce processus n'apparaît pas être une solution à tout, puisqu'**avoir plus de connaissances et/ou de compréhension ne conduit pas forcément à un comportement plus sûr en ligne**. En effet, les utilisateurs les plus avancés n'ont pas nécessairement toujours de meilleures pratiques de sécurité, ne prennent pas toujours les mesures de protection adéquates, ou ne font pas toujours attention, ce qui peut s'avérer dangereux et les exposer plus que les utilisateurs inexpérimentés.[11, 18]

En outre, beaucoup d'utilisateurs déclarent comprendre les menaces, mais ne font rien pour s'en protéger ou bien peuvent avoir l'intention d'adopter un comportement spécifique, mais sans passer à l'action (par exemple, l'intention de choisir un mot de passe sécurisé, tout en continuant d'utiliser un mot de passe faible.) [11, 26]

Enfin, **une compréhension adéquate des risques ne favorise pas automatiquement la prise de conscience des techniques adaptées** pour s'en protéger. Et faire l'effort de devoir se tenir à jour face aux évolutions rapides et constantes des technologies peut paraître insurmontable pour des personnes n'ayant pas de connaissances poussées — et ne souhaitant pas les acquérir, produisant ainsi une perception négative de la sécurité.[4, 17]

Sources de conseils

La perception des risques est façonnée par les informations auxquelles les personnes sont exposées, ce qu'ils croient et ce qu'ils ont vécu. **Les sources de conseils ont aussi une influence sur les comportements de sécurité et de confidentialité, la prise de décision et le comportement, notamment lorsqu'il s'agit de lancer une action**. Généralement, les utilisateurs suivent les conseils de personnes auxquelles ils font confiance et alignent leurs comportements sur des proches ou des personnes qui sont perçues comme ayant plus d'expérience dans le domaine informatique, même si rien n'indique que ces derniers offrent des conseils de qualité.[4, 8, 26]

Communication des risques

La communication des risques peut renforcer involontairement la perception inexacte des risques. Souvent, les systèmes de sécurité informatique tentent de communiquer les risques associés aux prises de décisions, mais c'est généralement inefficace, notamment parce que les utilisateurs peuvent s'habituer à ces messages et ne plus y prêter attention. Parfois, **les informations fournies sur les conseils de sécurité sont insuffisamment justifiées**, par exemple lorsqu'on n'explique pas pourquoi les mises à jour sont importantes et pourquoi il faut les faire régulièrement.

Finalement, l'efficience de la communication des risques repose non seulement sur la nature du risque, mais aussi sur l'alignement entre le modèle mental du risque de l'utilisateur et le modèle conceptuel sur lequel se base la communication des risques. Toutefois, **il existe un écart important entre les modèles mentaux des non-experts et des experts en sécurité, ce qui nuit à la communication efficace des risques**. Les utilisateurs vont accorder de l'importance à certains dangers et considérer certains conseils comme très efficaces bien que ce ne sont pas ceux privilégiés par les experts [4, 11, 20, 27, 28]

Les calculs et les compromis

Une autre approche examine les choix que font les individus et qui leur semblent rationnels, c'est-à-dire le calcul coûts-bénéfices.[15]

Considérer les bénéfices et avantages

Les bénéfices et avantages perçus influencent grandement la perception de la sécurité et des risques. Souvent lorsque les utilisateurs agissent en apparence dangereusement, c'est parce qu'ils recherchent des avantages, les activités à hauts risques étant associés à plus de bénéfices et avantages.[11, 14]

Généralement, les utilisateurs ont connaissance des coûts et des avantages impliqués, mais les perçoivent différemment, certains y voyant des avantages supérieurs à ne pas suivre les comportements préconisés plutôt qu'à se conformer aux politiques de sécurité. Ainsi, **suivre les conseils de sécurité est simplement perçu comme trop coûteux par certains, qui peuvent avoir une plus grande confiance en leurs propres mécanismes de sécurité et se méfier de ce qu'on leur propose**. Fréquemment, les bénéfices personnels éprouvés ont plus d'importance que le gain de sécurité hypothétique pour les utilisateurs qui ne suivent pas les conseils prodigués[15, 29, 30]

Considérer les coûts et conséquences

On doit considérer les coûts découlant des stratégies de gestion des risques, puisque ceux-ci augmentent les réticences des utilisateurs à suivre les conseils et à se protéger. **Les coûts induits par le respect des politiques et mesures de sécurité peuvent être d'ordre financier, cognitif, d'opportunité, de temps, d'effort ou d'accès aux avantages voulus**.[24]

Les utilisateurs peuvent être enclins à ignorer les conseils, ne voyant pas leur nécessité. Ils peuvent percevoir généralement plus d'avantages à maintenir les approches existantes. Les conséquences peuvent sembler hypothétiques et abstraites et donc difficiles à évaluer. **Les individus peuvent aussi remettre en question l'efficacité d'une protection offerte par rapport au coût associé** (par exemple, « pourquoi donnerais-je de l'argent, est-ce que ça me protège vraiment ? »). Finalement, on observe un problème d'asymétrie de l'information où les solutions gratuites et simples vont être privilégiées, car les usagers ne peuvent que difficilement distinguer la qualité des solutions proposées.[4, 11, 15, 24]

Considérer l'effet temporel

Un autre élément qui fait varier les perceptions du risque est l'aspect temporel dans lequel s'inscrit le risque (immédiat, futur, proche et lointain). L'effet du temps est une théorie selon laquelle **« la distance temporelle change les réponses aux événements futurs en changeant la façon dont les gens représentent mentalement ces événements »**.[5] Un danger sera perçu comme élevé s'il est immédiat et inversement, le risque perçu est réduit lorsque les conséquences négatives sont retardées ou sont susceptibles de l'être, mais aussi quand les effets positifs sont immédiats. Ainsi, les utilisateurs peuvent se mettre en danger dans certaines situations qui ne les amèneraient pas à percevoir de conséquences négatives immédiates, mais juste les avantages de leurs comportements (par exemple, choisir un mot de passe pratique qui réduit la charge cognitive immédiate, mais augmente les risques de piratage futurs).[1]

Rejet de sécurité — un mauvais compromis coûts-avantages

Selon certains chercheurs, le rejet des conseils de sécurité par les utilisateurs est une attitude rationnelle puisque **les experts qui les offrent surestiment leur valeur et les avantages qu'ils procurent, ignorant leurs coûts pour les utilisateurs** (notamment en temps et en efforts). Bien que les conseils soient adéquats techniquement, les coûts réels indirects qu'ils engendrent sont trop élevés en comparaison des préjudices potentiels directs contre lesquels on veut les protéger et les bénéfices sont souvent perçus comme étant théoriques par l'utilisateur. Cela aura souvent pour conséquences un boycottage de la sécurité et/ou des stratégies imparfaites qui sont censées la renforcer.[11, 15, 22, 23, 24, 31]

Considérer les compromis faits avec la sécurité

Les utilisateurs font souvent des compromis lorsqu'il s'agit de sécurité informatique, avec le temps, l'argent, les capacités ou la commodité. Certains peuvent être motivés par l'atout de sécurité qu'offre un dispositif (p. ex., une authentification à deux facteurs), alors que pour d'autres, la motivation principale sera la commodité d'utilisation. **La commodité perçue est donc importante à considérer, puisque celle-ci peut primer sur les préoccupations de sécurité**, les gens souhaitant des mécanismes et dispositifs simples avec une sécurité convenable selon leurs critères.[5, 15]

Quelques recommandations

Pour accroître la perception du risque, agir sur les perceptions et communiquer

Travailler à partir des stratégies d'adaptations des utilisateurs en essayant de les rendre plus sécurisées et de limiter leurs conséquences négatives. Par exemple, les stratégies d'adaptations sont courantes pour les mots de passe, comme la réutilisation. Dans ce cas, les gestionnaires de mots de passe pourraient être conçus pour faciliter la réutilisation sécurisée.[22]

Porter une attention toute particulière à la conception des interfaces et technologies que l'on propose et avec laquelle l'utilisateur interagit. Celle-ci peut influencer la compréhension de la sécurité, mais aussi l'expérience de l'utilisateur et donc ses perceptions de la sécurité et des risques.

Des avertissements efficaces doivent **énoncer les risques avec clarté** et les instructions doivent faciliter la compréhension et l'évitement des dommages.[24]

Présenter les informations de manière **attrayante et concise**, utiliser un langage simple et naturel[20]

Augmenter l'auto-efficacité des utilisateurs avec des outils, **développer la confiance des utilisateurs quant à leur capacité de sécurisation de leurs données et appareils**[17, 32] en offrant des conseils pratiques pour lesquels les usagers auront confiance que les résultats attendus se produiront.

Utiliser le pouvoir des émotions, car elles font partie intégrante des perceptions et appréciations de la sécurité et des risques.

Considérer la temporalité des conséquences, qu'elles soient réelles, directes, immédiates et sur le long terme, par exemple concernant les pratiques de réutilisation du mot de passe.[22]

Penser aux modèles mentaux des utilisateurs et non pas des experts pour communiquer les risques.[28]

Se focaliser sur les dangers qui peuvent avoir des conséquences négatives importantes, mais qui sont perçus comme moins risqués.[1]

L'éducation et la sensibilisation, oui, mais pas que…

Ne pas dépenser trop en essayant d'éduquer les utilisateurs sur certains sujets, comme les mots de passe, car beaucoup savent ce qu'est un bon mot de passe, même si peu mettent leurs connaissances en pratique. On pourrait plutôt choisir de sensibiliser les personnes aux différentes alternatives existantes, comme le gestionnaire de mot de passe par exemple.[5]

Éduquer ceux qui manquent de connaissances sur les risques et dangers, mais en adaptant la communication efficacement, notamment avec des messages persuasifs qui communiquent très concrètement les risques auxquels les usagers et l'organisation dont ils font partie sont confrontés, et les impacts négatifs concrets de ces risques sur l'organisation en question. Cela implique une certaine transparence plutôt que des messages où les risques restent très abstraits, afin de permettre aux utilisateurs de juger si le risque et acceptable ou non.[1, 17, 20]

La personnalisation des politiques de sécurité et des outils que l'on offre peut participer à des comportements plus sûrs en modifiant la perception de la sécurité.

- Éduquer en communiquant des messages et exemples personnalisés des risques et les conséquences directes des choix des utilisateurs. Faire ressentir une perte personnelle par exemple
- Personnaliser — notamment les boîtes de dialogues qui présentent les décisions de sécurité lorsqu'il y en a, car celles existantes sont généralement ignorées et inefficaces.[11, 16, 20]

- Éduquer sur les expériences biaisées et les informations inexactes.[6]

Considérer ce que l'on propose à partir des avantages et des inconvénients pour les utilisateurs

Utiliser la rétroaction pour pouvoir comprendre ce que les gens estiment contraignant et lourd, pour identifier les éventuelles difficultés ou coûts auxquels ils pourraient être confrontés, ce qu'ils seraient prêts à faire, ainsi que tout ce qui peut impacter négativement leurs perceptions et utilisations. C'est aussi important si l'on veut offrir des informations complètes ou porter leur attention sur un risque particulier.[26]

Considérer ce qui peut être à la fois important aux yeux des utilisateurs, mais également problématique en sécurité, comme les compromis avec la commodité ou la facilité d'utilisation, pour motiver un comportement plus sûr et atténuer les perceptions négatives. D'autant plus que les utilisateurs tronqueront souvent la sécurité pour la commodité, la sécurité n'étant pas toujours un objectif premier.[5, 15, 24]

Considérer les dommages — comprendre que les utilisateurs subissent souvent plus une perte de temps que d'argent.[24]

Penser à ce que l'utilisateur trouvera utile, nécessaire ou efficace, car s'il n'a pas cette perception, il résistera à la mise en œuvre des recommandations.[31]

Mettre en évidence les risques et les avantages des comportements de protection et travailler sur l'écart de perception concernant les avantages à adhérer aux conseils de sécurité. [1, 15]

Éliminer les conseils qui ne sont plus pertinents pour éviter le cumul des conseils qui entraîne un rejet de la sécurité, perçue comme un fardeau. [24]

Sélectionner les conseils, leur donner un ordre de priorité d'autant plus que les utilisateurs font des sélections entre les recommandations qu'ils ignorent et celles qu'ils adoptent. [24]

Automatiser si possible les actions protectrices qui peuvent l'être, ou les rendre aussi simples que possible, pour soulager la charge qui leur est imposée et qui peut nourrir des perceptions négatives de la sécurité.[11]

Références

[1] Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547-559.

[2] Kouabenan, D. R. (2012). Décision, perception du risque et sécurité. In Traité de Psychologie du Travail et des Organisations(pp. 281-322). Dunod.

[3] https://www.larousse.fr/encyclopedie/divers/perception/78270 :

[4] Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). « I've Got Nothing to Lose » : Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018) (pp. 197-216).

[5] Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233-244

[6] Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception?. Risk analysis, 2(2), 83-93.

[7] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208-220.

[8] Furnell, S., Clarke, N., Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users?. Information Management & Computer Security.

[9] Sjöberg, L. (2000). Factors in risk perception. Risk analysis, 20(1), 1-12.

[10] Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H., & Felten, E. (2002, April). Users' conceptions of risks and harms on the web: a comparative study. In CHI'02 extended abstracts on Human factors in computing systems (pp. 614-615).

[11] Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012, May). The psychology of security for the home computer user. In 2012 IEEE Symposium on Security and Privacy (pp. 209-223). IEEE.

[12] Hogarth, R. M., Portell, M., Cuxart, A., & Kolev, G. I. (2011). Emotion and reason in everyday risk perception. Journal of Behavioral Decision Making, 24(2), 202-222.

[13] Böhm, G., & Brun, W. (2008). Intuition and affect in risk perception and decision making.

[14] Slovic, P., & Peters, E. (2006). Risk perception and affect. Current directions in psychological science, 15(6), 322-325.

[15] Fagan, M., & Khan, M. M. H. (2016). Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 59-75).

[16] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A., & Yamada, A. (2017, May). Self-confidence trumps knowledge: A cross-cultural study of security behavior. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems(pp. 2202-2214).

[17] Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs, 43(3), 449-473.

[18] Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 39-52).

[19] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553-567). IEEE.

[20] Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014, April). Using personal examples to improve risk communication for security & privacy decisions. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 2647-2656).

[21] Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies, 69(12), 870-883.

[22] Stobert, E., & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In 10th Symposium On Usable Privacy and Security ({SOUPS} 2014) (pp. 243-255).

[23] Wash, R. (2010, July). Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security (pp. 1-16).

[24] Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on New security paradigms workshop (pp. 133-144).

[25] Chiasson, S., Forget, A., Biddle, R., & Van Oorschot, P. C. (2009). User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, 8(6), 387.

[26] Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410-417.

[27] Vaniea, K. E., Rader, E., & Wash, R. (2014, April). Betrayed by updates: how negative experiences affect future security. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2671-2674).

[28] Asgharpour, F., Liu, D., & Camp, L. J. (2007, February). Mental models of security risks. In International Conference on Financial Cryptography and Data Security (pp. 367-377). Springer, Berlin, Heidelberg.

[29] Paul, C. L., Morse, E., Zhang, A., Choong, Y. Y., & Theofanos, M. (2011, September). A field study of user behavior and perceptions in smartcard authentication. In IFIP Conference on Human-Computer Interaction (pp. 1-17). Springer, Berlin, Heidelberg.

[30] Althobaiti, M. M., & Mayhew, P. (2014, October). Security and usability of authenticating process of online banking: User experience study. In 2014 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[31] Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 327-346).

[32] Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014, June). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In International conference of design, user experience, and usability (pp. 229-239). Springer, Cham.

[33]https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-159?rskey=FkcRCi&result=159

[34] Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics (pp. 235-251). Academic Press.