COTEC
FONDAZIONE PER L'INNOVAZIONE

Rischio Digitale e Percezione della Sicurezza

In collaborazione con

LINK UNIVERSITY CAMPUS

RISCHIO DIGITALE E PERCEZIONE DELLA SICUREZZA

Riccardo Viale

(Behavioral Insights Bicocca, Università di Milano Bicocca)

Davide Pietroni

(Dipartimento di Neuroscienze - Università D'Annunzio di Chieti)

Indice

Introduzione

Viviamo in una società che, attraverso norme sempre più dettagliate e tecnologie automatiche sempre più pervasive, persegue il raggiungimento della sicurezza e della certezza. L'attività legislativa cerca di coprire l'intera gamma dei comportamenti umani ed evitare in tal modo la terra di nessuno per il *freeriding*, le azioni antisociali e contro il bene pubblico. La tecnologia è orientata ad aiutare l'uomo a raggiungere tutti gli obbiettivi che si prefigge con la maggior facilità e certezza. Siamo nell'epoca della sicurezza e certezza? Il contrario.

Se il nostro nuovo secolo deve essere caratterizzato in qualche modo l'aggettivo migliore è l'incertezza. Se il secolo XX poteva essere quello del rischio, cioè della credenza diffusa a livello accademico e della gente comune di potere prevedere il futuro con stime affidabili di probabilità, oggi la complessità indotta dalla legislazione e dalla tecnologia rende questa speranza meno sicura. Il paradosso è stringente: aumentando le opportunità di relazione, di comunicazione, di informazione e di transazioni consentite dalle nuove tecnologie, in primis dal web, aumentano parallelamente le possibilità di distorsione, appropriazione indebita e violazione di queste funzioni.

Falsità della informazione, furto dei dati e delle immagini, pirateria nelle transazioni e violazione della privacy sono solo alcuni dei fenomeni crescenti che stanno riducendo sempre di più il livello della sicurezza dell'utente. Il fenomeno è ancora più macroscopico perché la dimensione psicologica di percezione della insicurezza è molto superiore di quella reale. Le reali violazioni e trasgressioni nel web sono, cioè, inferiori al percepito dall'utente. La Ecochamber del web tende ad ingigantire nel bene e nel male qualsiasi fenomeno veicolato al suo interno. Quindi anche la percezione del rischio sulla sicurezza tende ad ingigantirsi in modo irrazionale ed inconsapevole.

1. Cos'è il rischio?

La **percezione del rischio** influenza le nostre decisioni ed i nostri comportamenti quotidiani. Percepire un rischio significa valutare una possibile minaccia e tentare di comprenderne le conseguenze immediate e future sia sul piano razionale che su quello emozionale. Esiste una differenza fra rischio oggettivo e rischio soggettivo.

Il rischio oggettivo è calcolato solitamente da esperti in base alla *casistica* della serie storica degli eventi accaduti nel tempo.

Solitamente le persone non calcolano il rischio oggettivo, ma fanno comunque delle valutazioni per decidere come comportarsi con il risultato di una possibile *sovrastima* o *sottostima* rispetto al rischio oggettivo. Queste valutazioni, spesso distorte, vengono definite "rischio soggettivo".

Formalmente il rischio è il frutto della seguente semplice equazione:

Rischio = probabilità di un evento x entità dell'evento stesso

Probabilità: probabilità che si verifichi un danno

Entità: gravità del danno

Le caratteristiche del rischio che influenzano la sua percezione in rapporto alla sicurezza nel mondo digitale sono legate alla seguente serie di attributi (taluni definiti da due polarità) che caratterizzano la percezione del rischio:

- *comune vs terrificante*
  - in base all'intensità e valenza della emozione che suscita
  - più è terrificante, più viene percepito come rischioso (per es. avere il proprio account hackerato e messo nella lista dei fruitori dei siti pedofili)
  - questa è la caratteristica maggiormente predittiva nel determinare la percezione del rischio
- *controllo personale del rischio*
  - avere la sensazione di poter controllare personalmente un rischio ne diminuisce la percezione di gravità (per es. se posso gestire facilmente la mia password percepisco di meno il rischio che possano rubarmela)
- *volontarietà del rischio*
  - le persone tendono ad accettare rischi più elevati se li assumono volontariamente (per es. se ho la volontà e un forte interesse al download di un sito a rischio di virus tendo a sottostimare il rischio di infezione) mentre se gli stessi rischi vengono invece imposti, gli individui li percepiscono più minacciosi
- *cronico vs catastrofico*
  - un evento è percepito tanto più catastrofico quando colpisce più persone assieme (per es. quando gli hacker lanciano un attacco alla istituzione in cui si lavora). E' un forte predittore dell'accettabilità e della percezione del rischio (bassa accettabilità per rischi potenzialmente catastrofici)
- *gravità delle conseguenze*
  - se la gravità potenziale dei danni è molto elevata le persone diventano insensibili al fatto che la probabilità che accada un incidente sia magari molto bassa (per es. la perdita di tutti i dati nel proprio computer pur essendo molto bassa è valutata molto rischiosa)
- *effetto di immediatezza*
  - alcune attività sono considerate poco rischiose perché i benefici sono "immediati", mentre gli effetti dannosi sono "differiti" nel tempo (per es. l'assuefazione all'utilizzo degli strumenti digitali e soprattutto dei social network che genera gratificazioni immediate al costo di tempo sprecato per la formazione culturale, professionale e per i rapporti umani)
- *osservabilità*

  tanto più l'evento riesce a esser rappresentato attraverso una immagine concreta e vivida, tanto più temibile esso risulterà agli occhi delle persone (per es. la rappresentazione visiva dei virus fatta da alcuni programmi antivirus)

- *conoscenza del rischio*
  - la conoscenza può determinare due effetti speculari
  - effetto positivo: più ritengo di conoscerlo e più lo giudico rischioso (per es. conoscere i rischi del furto di dati e password)
  - effetto negativo: meno ritengo di conoscerlo e più lo giudico rischioso (per es. non conosco le modalità con cui alcune società costruiscono i miei profili psicologici dai dati del social network e possono manipolare le mie scelte politiche)
- *novità*
  - alcune attività, sostanze o tecnologie incutono timore perché sono nuove (per es. la comparsa nel web di nuovi virus)
- *grado di esposizione*
  - l'elevata esposizione personale e collettiva è associata ad alti valori di rischio (per es. l'utilizzo massivo del web e la dipendenza psicologica da parte dei giovani o la presenza di una estesa infezione virale che azzera i dati personali)

2. Specificità del Rischio Digitale

Le caratteristiche del rischio digitale possono venire raggruppate in due grandi fattori:

rischio terrificante

- rischi giudicati terrificanti, non controllati, catastrofici, con gravissime conseguenze, che minacciano le generazioni future, che sono assunti non volontariamente e a cui siamo personalmente e collettivamente esposti

rischio sconosciuto

- rischi giudicati non osservabili, non conosciuti, nuovi, con effetti differiti nel tempo, non conosciuti dalla scienza

Sulla base di questa descrizione si può creare una **mappa cognitiva del rischio digitale** frutto della sintesi del giudizio collettivo delle persone su una vasta serie di rischi. Conoscere la posizione in questa mappa di uno specifico rischio in relazione ad altri rischi permette di capire come mai le persone hanno a volte reazioni molto forti verso rischi innocui, mentre talvolta hanno reazioni molto blande verso rischi noti.

2.1 Valutazione del rischio digitale

Si possono identificare due approcci allo studio della percezione del rischio digitale:

- tracciare un *profilo individuale* delle ragioni che sottostanno alla percezione di uno specifico rischio sulla base delle particolari caratteristiche di quel rischio
- studiare i *meccanismi generali* che sottostanno alla valutazione del rischio

E' ormai riconosciuta da molti studiosi l'importanza delle emozioni e sentimenti viscerali nella valutazione del rischio. Ne sono derivati alcuni modelli di percezione del rischio che di seguito vengo sinteticamente illustrati.

Euristica affettiva: per decidere la pericolosità di un rischio, le persone consultano *l'emozione associata alle immagini* che hanno nella memoria riguardo a quel specifico rischio.

Solitamente si ha una relazione inversamente proporzionale tra rischio e beneficio, mediata dall'euristica affettiva. Ovverosia più le attività sono percepite come piacevoli e fonte di benefici (ad esempio condividere molte foto personali con gli amici attraverso la rete) più i rischi ad essi associate vengono percepiti limitati, ciò in contraddizione con la logica fattuale che delinea una correlazione positiva tra benefici di una attività e rischi che essa comporta (si pensi ad esempio allo sfruttamento per la produzione energetica della scissione dell'atomo).

Collegati alla componente affettiva vi sono vari meccanismi fonti di errori e distorsioni nelle valutazioni e nei giudizi fra cui:

- **l'euristica della disponibilità**: un evento è giudicato più frequente quanto più è facile immaginarne degli esempi. Non sempre però la disponibilità è legata alla frequenza oggettiva degli eventi. Spesso essa è più influenzata dagli aspetti emozionali veicolati dalla comunicazione digitale e dai mass media. Si pensi ai vari fenomeni di etichettamento emozionale come la "mucca pazza" piuttosto che gli OGM o, nel mondo digitale, i virus.
- **l'illusione di controllo**: questa illusione determina una serie di fenomeni
    - *sovrastima delle probabilità di successo* legate alla propria performance
    - *sottostima del peso del caso*
    - ritenere di avere maggiore controllo sull'esito di quanto non sia in realtà
    - *forte impatto sulla percezione del rischio*, più penso di poter controllare una situazione, meno penso di essere a rischio

      Esempio: si percepisce meno il rischio di avere hackerato il proprio account quando siamo noi a decidere come proteggerci piuttosto che seguire le procedure automatizzate.

Bias ottimistico ovverosia la tendenza a *giudicare gli altri più esposti al rischio* di quanto lo siamo noi.

Ad esempio, ci giudichiamo meno vulnerabili al furto dei dati bancari e del denaro dal nostro conto rispetto alla media statistica del rischio.

Tale distorsione ottimistica è mitigata quando in nostro stato d'animo è negativo ed è la gravità percepita dell'evento. Al contrario la percezione di controllo ed il proprio livello di esperienza aumentano l'effetto del bias.

3. Cos'è la sicurezza digitale?

La sicurezza è un concetto speculare a quello di rischio. Esso ha una componente soggettiva ed oggettiva come il rischio. La sicurezza percepita è diversa dalla sicurezza oggettiva. Se ho una bassissima sicurezza percepita del rischio di borseggi in un'area a forte immigrazione irregolare ciò non vuol dire che la reale percentuale di borseggi corrisponda a questa percezione. Spesso non è così, come dimostrano alcune analisi sulla sovrapercezione della percentuale di immigrati in Italia rispetto ai dati reali. La sicurezza fa riferimento a fenomeni che hanno a che fare con il benessere della nostra persona. Possono essere legati alla propria incolumità, alla salute, alla condizione economica, ai rapporti sociali, a quelli affettivi, e così via.

Il tema della sicurezza diventa rilevante quando questi valori e condizioni sono messi in pericolo. Il rischio sicurezza è quindi la probabilità che questo stato di benessere e protezione non sia più garantito, e che l'assenza o l'indebolimento dello stesso possa rappresentare un danno per la persona. Nel campo digitale la sicurezza ha a che fare con una serie di fenomeni:

- Privacy: il pericolo che la propria vita privata e le proprie comunicazioni e foto siano rubate e diffuse nel web
- Protezione dati: l'acquisizione fraudolenta dei dati personali sensibili dal web
- Furti: l'utilizzo delle password bancarie per transazioni fraudolente dai propri conti correnti
- Benessere: la dipendenza e la assuefazione all'uso degli strumenti digitali e delle piattaforme web
- Immunità antivirale: il rischio di infezioni virali che contaminino i propri device e cancellino o ne alterino le memorie e le funzionalità
- Computer failure: il collasso del device per malfunzionamento dell'hardware

La letteratura prevalente sulla sicurezza digitale ha analizzato la sicurezza percepita nell'e-commerce (si veda appendice A). Ad esempio Salisbury et al (2001) hanno studiato l'importanza relativa della sicurezza in rapporto alla facilità e al valore percepito di utilizzo nel convincere le persone ad acquistare attraverso l'e-commerce. I risultati statistici mostrano come una più alta sicurezza percepita del web causi una maggiore intenzione a comprare usando siti di e-commerce B2C rispetto al ruolo della utilità e facilità percepita. Cheng et al (2006) hanno dimostrato risultati simili sulla sicurezza percepita del web. Lian e Lin (2008) hanno mostrato come la sicurezza percepita insieme ad altri fattori come la propensione personale alla innovazione, le preoccupazioni per la privacy ed il coinvolgimento personale nel prodotto sia un fattore determinante nel condizionare le attività di shopping on line. Chang e Chen (2009) hanno confermato empiricamente il dato insieme alla evidenza dell'importanza della qualità dell'interfaccia come determinante della fedeltà all'utilizzo dell'e-commerce. Cheung e Lee (2006) hanno dimostrato come la sicurezza percepita del web sia determinante per mantenere un buon livello di fiducia e fedeltà nello shopping on line. La sicurezza percepita si associa ad una bassa percezione del rischio nelle transazioni e ad un sentimento di fiducia e protezione dai pericoli.

Nel loro studio Hartono et al (2014) individuano quattro dimensioni focali della sicurezza percepita (si veda Appendice B) che sono condivise dalla maggior parte degli studiosi:

1) Riservatezza: si riferisce al grado in cui si viene salvaguardati da disclosure indesiderate delle informazioni personali. "Encryption" e altre forme digitali di autenticazione rafforzano tale percezione di riservatezza.
2) Integrità: si riferisce al grado con cui viene evitata una modifica inopportuna delle informazioni scambiate. Firme digitali e programmi anti virus aumentano la percezione di integrità.
3) Disponibilità: si riferisce al grado con cui l'informazione è prontamente disponibile quando richiesta dalle persone autorizzate ad accedervi. Sistemi di Back-up aumentano la percezione di disponibilità.
4) Non-repudation (non sconfessione): si riferisce al grado in cui il sistema è capace di assicurare che l'informazione inviata dal compratore sia ricevuta dal venditore autorizzato, e che quest'ultimo non neghi successivamente la transazione avvenuta. La firma digitale è una misura che aumenta la percezione della non sconfessione.

In sintesi (si vedano appendici C e D) la percezione della sicurezza digitale è proporzionale a quanto l'utente ritiene che le sue informazioni non vengano rese pubbliche, che esse non vengano alterate da soggetti non autorizzati, che il veditore sia disponibile a fornire tutta l'informazione richiesta dal compratore e che il venditore sia veramente il soggetto che afferma di essere e che non possa successivamente sconfessare la transazione. Questa sicurezza percepita ha un impatto positivo sulla facilità e sulla utilità percepita aumentando in tal modo la fedeltà del consumatore al sito di B2C.

Appendice A. Rassegna sulle definizioni di sicurezza digitale

Studi	Definizioni
Salisbury et al. [66]	The extent to which one believes that the Web is secure for transmitting sensitive information
Cheng et al. [19]	
Liao and Wong [48]	
Cheung and Lee [20]	The perception of Internet shoppers of Internet merchants' ability to fulfill security requirements
Cheung and Lee [21]	The subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations
Chellappa and Pavlou [18]	
Liu et al. [50]	The perception that making a transaction with an Internet store is safe
Yenisey et al. [80]	The level of security that users feel while they are shopping on e-commerce sites
Fang et al. [28]	The extent to which a user believes that using a particular application will not expose his or her private information to any unauthorized party
Lian and Lin [47]	One's awareness of Web security when providing and sending personal or financial information
Flavian and Guinaliu [29]	The subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations

Chang and Chen [17]	Customer perceptions of the security of the transaction as a whole
Roca et al. [64]	The customers' perception of the degree of protection against a threat that creates a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, modification of data, denial of service, and/or fraud, waste and abuse
Yousafzai et al. [81]	The customers' perception of the degree of protection against destruction, disclosure, modification of data, fraud, and abuse
Kim et al. [46]	The customer's subjective evaluation of the system's security

Appendice B. Rassegna sulle dimensioni della sicurezza digitale

Studies	Dimensions of security
Bodin et al. [11]	Confidentiality, integrity, availability
Ryan and Ryan [65]	
Erlich and Zviran [27]	
Berghmans and Van Roy [9]	
Gordon et al. [34]	
Dube et al. [26]	
Ransbotham et al. [63]	
Siponen and Kukkonen [70]	Confidentiality, integrity, availability, non-repudiation
Cegielski [16]	Confidentiality, integrity, availability, authentication, non-repudiation
Vaidyanathan and Mautone [77]	
McFadzean et al. [52]	Confidentiality, integrity, availability, authentication, access control, non-repudiation
Parent [59]	
Gurbani and McGee [35]	Confidentiality, integrity, availability, authentication, access control, non-repudiation, communications security, privacy

Appendice C. Rassegna sulle misure della sicurezza digitale

Studi	Indicators of perceived information security
Salisbury et al. [66]	1. I would feel secure sending sensitive information across the World Wide Web
Cheng et al. [19]	2. The World Wide Web is a secure means through which to send sensitive information
Vatanasombut et al. [78]	3. I would feel totally safe providing sensitive information about myself over the World Wide Web
Chang and Chen [17]	4. Overall, the World Wide Web is a safe place to transmit sensitive information
Cheung and Lee [20]	1. Internet vendors implement security measures to protect Internet shoppers

	2. Internet vendors have the ability to verify Internet shoppers' identity for security purposes
Cheung and Lee [21]	3. Internet vendors usually ensure that transactional information is protected from being accidentally altered or destroyed during transmission on the Internet
Chellappa and Pavlou [18]	1. The degree of confidence that information will only reach the appropriate party 2. The degree of confidence that inappropriate parties would neither view nor store consumer information 3. The degree of confidence that the retailer will not expose consumer information to others 4. The degree of confidence that inappropriate parties will not manipulate consumer information during transaction 5. The degree of overall confidence in the transaction's security
Liu et al. [50]	1. I believe that shopping on this Internet store is just as safe as placing an order by phone 2. It is just as safe to make a credit card purchase at this Internet store as it is to make one in person 3. The data transmission between my computer and this Internet store is safe 4. This Internet store is capable of preventing illegal access
O'Cass and Fenech [57]	1. I feel secure sending personal information across the Web 2. I feel safe providing personal information about me to Web retailer
Lian and Lin [47]	3. Web is a safe environment to provide personal information
Yenisey et al. [80]	1. I believe the information I provide with SNS will not be manipulated by inappropriate parties
Shin [69]	2. I am confident that the private information I provide with SNS will be secured. 3. I believe inappropriate parties may deliberately view the information I provide with this SNS
Fang et al. [28]	1. I feel secure to perform this task on the handheld computer 2. There is feedback indicating the information is protected
Flavian and Guinaliu [29]	1. I think this website has mechanisms to ensure the safe transmission of its users' information 2. I think this website shows great concern for the security of any transactions 3. I think this website has sufficient technical capacity to ensure that no other organization will supplant its identity on the Internet 4. I am sure of the identity of this website when I establish contact via the Internet
	5. When I send data to this website, I am sure that they will not be intercepted by unauthorized third parties 6. I think this website has sufficient technical capacity to ensure that the data I send will not be intercepted by hackers 7. When I send data to this website, I am sure they cannot be modified by a third party 8. I think this website has sufficient technical capacity to ensure that the data I send cannot be modified by a third party

Liao and Wong [48]	1. The Internet e-banking systems restrict unauthorized access 2. The Internet e-banking systems protect customer private data 3. The Internet e-banking systems have rigorous security control
Roca et al. [64]	1. I think the online trading systems have sufficient technical capacity to ensure that the data I send cannot be modified by a third party 2. The online trading systems have enough security measures to protect my personal and financial information 3. When I send data to the online trading systems, I am sure that they will not be intercepted by unauthorized third parties 4. I think the online trading systems have sufficient technical capacity to ensure that no other organization will supplant its identity on the Internet
Yousafzai et al. [81]	1. I believe my Internet banking transaction information will not be lost during an online session 2. I believe my Internet banking transaction information will only reach the target bank account 3. While using Internet banking, I believe that the security system will confirm my identity before disclosing account information 4. While using Internet banking, I believe that the security system will confirm my identity before processing transactions 5. While using Internet banking, I believe that the security system does not allow unauthorized access to the account 6. While using Internet banking, I believe that the security system stops any unauthorized changes to a transaction 7. While using Internet banking, I believe that the security system provides a secure environment in which to bank
Shin [69]	1. In general, I feel secure in using IPTV system. 2. I feel safe in transaction, downloading contents (VoD), and accessing sites via IPTV. 3. IPTV is well built against security-related concerns such as hacking, unauthorized uses, theft of data, interception of transmission,and virus.
Kim et al. [46]	1. I perceive EPS as secure 2. I perceive the information relating to user and EPS transactions as secure 3. The information I provided in previous EPS is helpful for secure payment transactions4. I do not fear hacker invasions into EPS
Swilley [73]	1. I feel secure putting credit card information on my cell phone 2. I feel secure putting personal information, such as my driver's license number on a wallet phone. 3. I feel safe in my transactions with a wallet phone 4. I feel like my privacy is protected on a wallet phone 5. I feel I can trust having my information on a wallet phone

Appendice D. Indicatori dei Costrutti

Tutti gli indicatori sono stati misurati su una scala Likert a 7 punti (da 1="assolutamente in disaccordo" a 7= "assolutamente d'accordo"). Ad ogni consumatore online era stato chiesto il livello con cui concordava con ciascuna delle seguenti affermazioni.

Costrutti	Indicatori
Perceived confidentiality	PC1. Someone uses my Internet ID to read my transactional information. [R]
	PC2. Someone uses my Internet ID to make order. [R]
	PC3. Someone steals my Internet ID. [R]
Perceived integrity	PI1. The site transmits my transactional information accurately. [D]
	PI2. My transactional information is altered. [R]
	PI3. The site records my transactional information incorrectly. [R]
Perceived availability	PA1. I cannot order due to system failure. [R]
	PA2. I cannot order due to database failure. [R] PA3. I cannot order due to network failure. [R]
Perceived non-repudiation	PNR1. This site uses digital signature
	PNR2. The legislation backs up the digital signature
	PNR3. The identity of this site is trustworthy
Perceived ease of use	EAS1. It is easy to place an order
	EAS2. It is easy to shop
	EAS3. It is easy to learn the shopping procedure
	EAS4. Everyone can easily master the shopping procedure
Perceived usefulness	USE1. This site is very informative
	USE2. I can easily find the product that I am looking for USE3. I can easily get the information that I need
Attitude	ATT1. It is a good idea to shop in this site
	ATT2. It is a smart idea to shop in this site
	ATT3. It is enjoyable to shop in this site ATT4. I feel positive to shop in this site

Intention	INT1. This site will be my first option whenever I want to shop INT2. I will use this site again INT3. I will use this site regularly INT4. I will use this site frequently
Perceived security (global indicators)	PS1. My personal information is securely managed in this site PS2. This site is safe for my personal information

[D] Indicatore eliminato.

[R] Indicatore rovesciato.

4. Focus Group sulla Sicurezza Digitale

Caratteristiche dei partecipanti

Il gruppo di partecipanti al focus group era composto da 5 maschi e 4 femmine. L'età media era 37 anni e le posizioni professionali erano le seguenti: 2 operatori, 3 impiegati e 4 ricercatori universitari. Le conoscenze in ambito ICT rilevate attraverso un breve test di profitto con 7 item a scelta multipla ha evidenziato una competenza medio-alta del campione (media = 4,55 risposte corrette; DS = 1,1). Il titolo di studio modale era la laurea magistrale.

4.1 Procedura

Dopo l'accoglienza e l'illustrazione sommaria degli obiettivi e della metodologia del focus group, si è somministrato un questionario sociodemografico e competenziale, dopo il quale si è intervenuti al fine di creare un clima informale, aperto e rilassato tra i partecipanti. Prima individualmente e poi in gruppo si è invitato a rievocare le proprie esperienze digitali critiche. Ci si è quindi focalizzati sulla elaborazione collettiva di una lista delle minacce digitali percepite come più ansiogene. Per ognuna si è proceduto a stimarne la probabilità, la pericolosità e la propensione ad investire del denaro (willingness to pay) al fine di tutelarsi da ogni specifica minaccia per la propria intera vita digitale. I partecipanti sono stati quindi invitati a rievocare specifici episodi personali o vicari in relazione a questa lista di minacce.

In ottica propositiva, i partecipanti sono stati infine invitati a riflettere su possibili contromisure utili a mitigare probabilità e gravità delle minacce, individuando quindi delle proposte funzionali a rendere più serena e positiva l'esperienza con le ICT.

4.2 Risultati

Prima di approfondire la riflessione sulle diverse possibili minacce, il gruppo ha attribuito mediamente una probabilità complessiva di circa il 55% di cadere prima o poi vittima di una "trappola" nel corso della propria vita digitale. La gravità media che attribuiva a questa evenienza (su una scala da 1 a 7) era percepita come molto elevata, ovverosia pari a 6. Infine, mediamente i partecipanti erano disposti a pagare una cifra pari a 325 euro per una polizza capace di proteggerli complessivamente dall'insieme di tutte le minacce individuate lungo la loro intera vita digitale.

Successivamente a queste valutazioni generali si è proceduto ad analizzare le percezioni specifiche relative ai diversi possibili incidenti digitali.

Le minacce individuate sono state 15 (tra parentesi indichiamo l'etichetta sintetica per futuri riferimenti): l'infezione da virus di pc e smartphone (virus), il furto di immagini catturate dalla webcam del proprio device (webcam), il furto dei codici homebanking (homabanking), l'accesso fraudolento al proprio account mail (mail), il furto dei codici di accesso ai social media (social), il furto di identità (identità), il furto di dati sensibili sui propri familiari (famiglia), il furto e l'uso non autorizzato di proprie immagini personali (immagini), la clonazione di bancomat e carte di credito (clonazione), il vedere il proprio ordine di acquisto/pagamento non riconosciuto dal venditore (ripudio), il furto di documenti e comunicazioni personali (documenti), l'essere coinvolti in "catene di Sant'Antonio" (catene), l'essere bombardati da spamming (spam), l'essere geolocalizzati contro la propria volontà (geolocal), il rischiare di essere esposti anche in momenti inopportuni da annunci pubblicitari di prodotti/servizi precedentemente consultati (retargeting).

Specificamente tra le 15 minacce quelle percepite come più gravi riguardavano identità, famiglia, social, documenti, immagini e web. Solo a livello intermedio sono state valutate le minacce relative a homebanking, virus, clonazione, mail e geolocalizzazione. Mentre erano percepite come meno gravi le minacce di ripudio, retargeting, catene e spam.

In termini di probabilità percepite delle diverse minacce, gli eventi ritenuti più probabili riguardavano lo spam, le catene, le immagini, la geolocalizzazione, i virus e il retargeting.

Gli eventi moderatamente probabili erano relativi invece a identità, homebanking, mail e ripudio.

Infine le minacce meno probabili riguardavano documenti, famiglia, clonazione e webcam.

Rispetto alla disponibilità a pagare per essere preservati da ciascun di questi rischi emerge che i partecipanti erano disponibili ad investire le cifre più alte per proteggersi da eventi relativi a homebanking (un partecipante arriva ad offrire 15.000 euro), identità (un partecipante arriva ad offrire 5000 euro), clonazione, documenti e famiglia. Un investimento moderato i partecipanti si dichiaravano propensi ad effettuarlo relativamente a mail, social, immagini, virus e geolocalizzazione. Mentre l'investimento era basso per la protezione da retargeting, ripudio, webcam, spam e catene.

Combinando le riflessioni sulle percezioni di probabilità e sulle percezioni di gravità delle diverse minacce è emerso con nettezza che la minaccia percepita come più insidiosa e pesante era quella relativa al **furto ed uso improprio delle proprie immagini personali.**

Questa evidenza è coerente con gli orientamenti aneddotici spontaneamente sviluppati dal gruppo.

4.3 Evidenze narrative

Stimolati a rievocare specifici episodi di eventi digitali percepiti come minacciosi per la propria privacy e sicurezza i partecipanti hanno generato le seguenti narrazioni.

Un docente ha raccontato una aggressione informatica al proprio account di posta elettronica, ha sottolineato lo stress ed il senso di impotenza nel non riuscire ad accedervi e nel sentirsi ripudiato dal gestore, ed il peso della consapevolezza di mettere a disposizione per fini

probabilmente fraudolenti una mole di dati sensibili. La situazione si risolse prontamente in giornata con la denuncia alla polizia postale ma la riattivazione dell'account fu velocemente ottenuta solo grazie all'intervento di un amico operante per il gestore. La chiosa ha sottolineato la drammaticità anche emotiva dell'esperienza "Avrei in quel momento pagato qualsiasi cifra per rientrare e recuperare i miei documenti, il danno che si potrebbe sviluppare è potenzialmente così alto che non c'è valore che potrebbe compensarlo". Dopo questa esperienza il partecipante ha cambiato operatore optando per uno che offrisse maggiori garanzie di sicurezza.

Un altro partecipante ha evidenziato un caso di uso fraudolento della propria carta di credito che comunque fu prontamente rilevato, bloccato e risolto. La chiosa è stata che questi eventi "non fanno paura perché alla fine c'è la banca che garantisce".

Alcuni partecipanti hanno rievocato casi di truffe nel commercio elettronico. In alcuni episodi l'aver notato delle domande improprie al momento dell'acquisto ha insospettato l'utente facendolo allontanare dalla transazione, in altri si è proceduto all'acquisto di beni e servizi su piattaforme come ebay e groupon per poi scoprire che il venditore aveva cessato l'attività, aveva cancellato il proprio profilo o comunque si era reso irreperibile. Solo a posteriori le vittime di questi incidenti avevano cercato sul web informazioni sul venditore e talvolta avevano trovato espliciti moniti. La tendenza del gruppo è apparsa quella di minimizzare la gravità psicologica ed emozionale di questi eventi "E' stata la classica sola, colpa mia che non ero esperto e non ho controllato i feedback del venditore. Mi sono semplicemente limitato a segnalare il fatto alla piatta forma e ho accettato la perdita di pochi euro. Mi è servito come esperienza."

Un partecipante esprimendo più ansia e disagio ha narrato il caso della perdita di una intera cartella con documenti di lavoro nel proprio driver causata dall'attacco di un virus contratto durante un momento di navigazione da casa. Fortunatamente i tecnici della sua azienda riuscirono a trovarne traccia e a ripristinarlo. Una seconda partecipante ha evidenziato un episodio simile presumibilmente causato dalla navigazione attraverso l'hotspot del telefonino, ma in questo caso i dati non si riuscì a recuperarli ed i tecnici mai compresero le cause della perdita.

Approfondendo la discussione sui possibili risvolti più inquietanti delle aggressioni digitali alla privacy, il gruppo ha evidenziato una utile distinzione concettuale tra danno prevalentemente economico e danno morale/sociale/emozionale. Questa polarizzazione è coerente con la dicotomia funzionale/espressivo che viene spesso impiegata per concettualizzare e categorizzare gli eventi significativi.

Il gruppo si è quindi spinto a sviscerare le implicazioni sul versante socioaffettivo evidenziando che esso è quello meno compensabile economicamente.

Qualcuno ha prontamente evidenziato, negli scenari più estremi, che a questo tipo di aggressioni digitali appartiene l'ambito talvolta drammaticamente fatale del cyber bullismo, spesso originato dalla diffusione non autorizzata di materiale audiovisivo molto sensibile. Un altro partecipante ha evidenziato come anche la sola diffusione di comunicazioni e riflessione personali, magari attraverso i social, possa creare pesanti disagi psicologici alla vittima.

Una partecipante ha affermato di avere talvolta provato un senso di stupore ed inquietudine quando la applicazione di navigazione del proprio device si è mostrata in grado di prevedere la destinazione del suo viaggio in auto anche quando quella meta fosse solo occasionale "Mi sono sentita controllata come nel Truman Show".

Altri partecipanti hanno sottolineato, al netto del danno economico risarcibile, il peso psicologico dello scoprire rubata la propria identità al fine di operare truffe ed altri atti illeciti a proprio nome con il conseguente stress dovuto al coinvolgimento in procedimenti penali.

Una partecipante ha definito come "incidente diplomatico familiare" fonte di stress e disagio l'episodio di retargeting su siti di compravendite immobiliari avvenuto mentre stava navigando affianco ad un congiunto a cui aveva garantito la sua intenzione di non cambiare casa.

Anche nella rievocazione di eventi critici è emerso, come sottolineato nel paragrafo precedente, il peso psicologico del furto e dell'uso improprio di immagini personali come incidente percepito contemporaneamente grave e probabile nonché capace di saturare le valenze potenzialmente emotivamente catastrofiche ed economicamente non compensabili della polarità morale/espressiva sopra descritta.

In particolare, un partecipante ha evidenziato il rischio di essere monitorati inconsapevolmente dalla webcam del proprio PC o addirittura del proprio smartphone, esponendosi ad inquietanti invasioni della privacy "vedono dentro casa mia e scoprono dove metto le cose preziose" o, sul versante professionale, a spionaggio industriale "viene in mente la foto di Zuckerberg al pc con un artigianale pezzo di scotch a coprire la webcam".

Una partecipante invece ha ricordato il caso di un amico che causalmente viene a scoprire che le sue immagini erano state utilizzate come foto del profilo di un altro utente che, pur presentandosi con un altro nome, utilizzava la sua faccia.

Ancora più emotivamente pesante il caso in cui una amica che scopre che le foto del proprio matrimonio erano state illecitamente usate in un profilo social. La partecipante ha messo in risalto il disagio emotivo associato al furto di immagini così emotivamente significative.

Le emozioni che il gruppo ha associato più frequentemente a questi episodi sono ansia, senso di insicurezza, paura e stupore generato dalla inconsapevolezza.

4.4 Cause e possibili rimedi

Quasi al fine di esorcizzare e mitigare il senso di impotenza e le ansie generate dalla produzione delle numerose e talvolta inquietanti evidenze narrative, il gruppo spontaneamente ha iniziato a riflettere sulle responsabilità degli utenti stessi nel loro rapporto troppo disinvolto col web nel creare le condizioni ideali per la concretizzazione delle minacce digitali.

Alcuni partecipanti hanno osservato che l'atteggiamento mentale leggero e ludico con cui tendenzialmente ci si approccia ai social media potrebbe determinare la sottovalutazione dei rischi di violazione della propria privacy. Alcuni utenti possono infatti spingersi a rendere pubbliche informazioni molto personali o comunque ingenue ("sono in vacanza per tutto il mese", "stasera sono a casa da sola"), fino ad arrivare a fornire il proprio indirizzo di casa.

Nonostante i partecipanti stessi abbiano ammesso di fare talvolta ricorso ai social media per raccogliere informazioni su potenziali collaboratori e studenti, e persino per decidere se dare o meno una opportunità lavorativa ("una mia amica ha annullato il colloquio di lavoro con una potenziale collaboratrice domestica perché nel suo profilo social postava foto troppo provocanti"), hanno confessato di non tenere sempre presente questa possibile evenienza quando decidono di postare foto e contenuti sul loro profilo.

Sempre in prospettiva autocritica, altri partecipanti hanno lamentato l'atteggiamento di leggerezza con cui si aprono diversi profili, anche professionali, di cui poi talvolta si dimentica persino l'esistenza lasciandoli ingestiti, non aggiornati ed incurati con il rischio di veicolare una immagine di sciatteria agli occhi di chi dovesse consultarli per farsi una idea sulle proprie qualità professionali.

Sul versante delle responsabilità sistemiche, i partecipanti hanno osservato come la tecnologia e le sue modalità di impiego a fini espressivi e comunicativi corra nettamente più veloce della legislazione che ambisca a regolamentarla e a mitigarne gli usi malevoli. Si tratta di fenomeni veloci dall'impatto e dalle evoluzioni imprevedibili.

Il gruppo è stato quindi spronato a proporre possibili soluzioni per rendere più serena, sicura e piacevole l'esperienza digitale cercando di neutralizzare le minacce discusse.

Un partecipante ha lamentato che i più potenti social media hanno forse sottovalutato il loro impatto sulla vita delle persone ed "invece di tante paginate di policy avrebbero potuto trovare con 4 semplici pagine il modo di spiegare chiaramente agli utenti come funzionano". La colpa principale di queste piattaforme sarebbe quindi quella di non aver investito per "educare" i propri utenti al fine di renderli consapevoli dei propri meccanismi. Secondo un altro partecipante sarebbe dovuta essere la legislazione ad imporre questo sforzo di trasparenza.

Sul versante più micro e quotidiano, una partecipante ha ammesso che le piace pensare che per proteggersi dalle minacce digitali alla propria immagine sia sufficiente condividere nei social informazioni "banali, evitando di esporsi in profondità".

In particolare, quando le applicazioni chiedono il consenso per accedere ai dati personali, diversi partecipanti hanno confessato la tendenza a pigiare "OK, OK, in modo automatico". Una proposta per rimediare a questa inconsapevole istintività alla autorizzazione è stata che i gestori stimolino la consapevolezza degli utenti fornendo loro maggiori informazioni.

Un partecipante ha fatto però notare che questo rimedio rischierebbe di rendere vischiosa e lenta la navigazione, quando invece gli utenti chiedono sempre più snellezza e velocità della fruizione. La metafora che qui il gruppo ha sembrato prediligere è quella dei bugiardini dei farmaci, più sono lunghi più nessuno li legge nonostante sia in gioco un valore centrale come quello della propria salute.

Una alternativa emersa potenzialmente agevole da implementare è che i gestori delle applicazioni almeno tentino di aumentare la attenzione e la consapevolezza degli utenti nel momento autorizzativo evitando di posizionare la finestra di dialogo al centro dello schermo (come tipicamente avviene per le comunicazioni più innocue come quelle di batteria scarica) ma che stimolino la attenzione degli utenti variando ogni volta in modo casuale il posizionamento della finestra in diverse aree dello schermo, magari accompagnandola con una vibrazione dello smartphone o con un bip del pc.

In ottica positiva, una partecipante ha dichiarato un atteggiamento positivo verso la propria profilizzazione commerciale "non mi dispiace che il sistema conosca i miei interessi ed i miei gusti per comunicarmi cose che mi piacciono".

Il confine da non valicare è quello dello spamming selvaggio e persecutorio, per mitigare il quale viene proposto di semplificare il processo di pulizia dai cookies, magari facilitandone la attivazione premendo un solo tasto.

Come altri possibili rimedi è emersa la utilità di applicazioni che occasionalmente randomizzino e modifichino le password, o che almeno agiscano come remind quando da troppo tempo non si variano o quando si scopra di utilizzare la stessa password per troppi diversi account.

4.5 Discussione

Confrontando le valutazioni elaborate dai partecipanti all'inizio e al termine dell'esperienza di approfondimento, rievocazione e discussione nel focus group emergono alcune interessanti riflessioni conclusive.

Nonostante la valutazione media della probabilità percepita di occorrenza della costellazione delle 15 minacce individuate sia risultata coincidere perfettamente con la iniziale valutazione globale della percezione della probabilità di cadere in una trappola digitale nel corso della propria vita (55 %), la willingness to pay che è stata espressa all'inizio del focus per una polizza a copertura dal complesso delle minacce digitali è risultata più che raddoppiata al termine della discussione (755 euro versus 325 euro).

Per quanto riguarda la elevata gravità percepita inizialmente dichiarata (6 su una scala a 7 punti), essa appare più bassa della media della percezione di gravità delle 15 minacce individuate (4,8). Sembra quindi probabile che quando all'inizio i partecipanti hanno valutato globalmente la gravità delle minacce digitali si siano focalizzati soprattutto sul cluster di quelle più catastrofiche che, come abbiamo sopra descritto, corrispondono essenzialmente a quelle che determinano un danno identitario/emotivo/psicosociale piuttosto che operativo/economico/funzionale. A questo cluster abbiamo visto appartengono il furto di identità, la violazione del profilo social, l'uso illecito delle proprie immagini e di quelle dei familiari.

La percezione di gravità di queste singole minacce corrispondeva sostanzialmente con la percezione globale inizialmente espressa dai partecipanti quando hanno cominciato a riflettere sul fenomeno della insicurezza nelle ICT. Ne deriva che questo cluster di minacce può definirsi come prototipico degli scenari più ansiogeni ed inquietanti che albergano nella mente degli utenti ICT minandone la serenità della esperienza digitale.

Infine, incrociando questo cluster di minacce prototipiche con la loro singola probabilità percepita di accadimento, è emerso con evidenza il primato della probabilità percepita del furto ed uso improprio delle proprie immagini rispetto alla probabilità media delle altre minacce del cluster (67% versus 51 %).

Possiamo quindi concludere che al fine di migliorare la qualità emozionale della esperienza digitale degli utenti aumentando il loro senso di controllo e sicurezza, si potrebbe proporre la creazione di applicazioni che, operando la "ricerca per immagini", siano in grado automaticamente di passare al setaccio la "identità digitale" dell'utente comparando tutte le immagini originali da egli pubblicate con le immagini presenti sul web al fine di individuare e segnalare prontamente casi di abuso o comunque di utilizzo non autorizzato.

Dalle evidenze emerse dal focus possiamo ipotizzare che l'utente che regolarmente si affidi ad una applicazione di questo tipo ricevendone rassicurazione rispetto alla diffusione delle proprie immagini solo in contesti autorizzati, potrebbe godere di una esperienza digitale più serena, aperta e fiduciosa.

5. Indagine sulla Percezione dei Rischi Digitali

5.1 Obiettivi della ricerca

Gli obiettivi della presente indagine sono molteplici e raggruppabili nelle seguenti cinque categorie.

a) Capitalizzare le risultanze del focus group sopra descritto misurando in modo strutturato e su un campione più ampio la percezione dei rischi associati ai 15 rischi digitali emersi, nonché la disponibilità a pagare per neutralizzare.
b) Rilevare eventuali effetti di subadditività (l'assegnare giudizi di probabilità inferiore a una descrizione impacchettata di un evento rispetto alla probabilità dei singoli elementi che lo costituiscono) e di sensibilizzazione confrontando la percezione globale dei rischi digitali prima, durante e dopo la riflessione analitica sulle loro 15 specifiche possibili fattispecie.
c) Far sperimentare ai partecipanti una concreta esperienza di abuso digitale, distinguendo un abuso di tipo prevalentemente "espressivo" (utilizzo non autorizzato delle proprie foto personali) da un abuso prevalentemente funzionale" (accesso non autorizzato alla propria mail professionale), al fine di monitorare le specifiche risposte emozionali dei partecipanti nella immediatezza di questo evento critico.
d) Indagare gli effetti delle due tipologie di abuso sulla percezione globale e specifica delle possibili minacce digitali e sulla disponibilità al pagamento di una assicurazione per neutralizzarle.
e) Monitorare gli atteggiamenti verso i possibili rimedi (emersi anch'essi dal focus group) alle diverse minacce digitali.

5.2 Caratteristiche del campione

Hanno partecipato alla indagine 49 collaboratori della Università Link Campus di Roma (18 maschi e 31 femmine), appartenenti quindi alla stessa popolazione da cui provenivano i 9 partecipanti al focus group preliminare.

Il campione era stratificato come segue: 5 dirigenti, 4 docenti, 32 amministrativi, 2 tecnici e 6 ricercatori. Rispetto alla popolazione inizialmente invitata a partecipare all'indagine il tasso di risposta è stato del 58%.

5.3 Procedura e strumento

I partecipanti sono stati invitati attraverso la loro mail istituzionale a compilare un questionario on line dopo essersi immedesimati nello scenario in cui venivano allertati da un amico collega rispetto alla scoperta sul web di un abuso che li vedeva protagonisti e di cui l'amico si era premurato di allegare uno screenshot a dimostrazione dell'incidente digitale.

Il questionario era composto da 72 domande e richiedeva circa 15 minuti per essere affrontato. Specificamente il questionario era organizzato nelle seguenti sessioni sequenziali:

- reazioni emotive alla sperimentazione dell'abuso digitale (9 item likert a 7 punti) e 3 item relativi alla percezione della sua gravità (a 7 punti), probabilità (risposta aperta) e disponibilità al pagamento per neutralizzarlo (risposta aperta);

- rilevazione “a priori” su 3 item della percezione globale del complesso delle minacce digitali in termini di loro gravità (a 7 punti), probabilità (risposta aperta) e disponibilità al pagamento per neutralizzarle (risposta aperta);
- misura specifica attraverso 45 item delle percezioni delle 15 minacce digitali in termini di loro gravità (a 7 punti), probabilità (risposta aperta) e disponibilità al pagamento per neutralizzarle (risposta aperta);
- monitoraggio degli atteggiamenti rispetto ai possibili rimedi alle minacce digitali attraverso 6 item di accordo/disaccordo (a 7 punti), 1 domanda aperta sui possibili suggerimenti e 2 domande aperte sulla disponibilità al pagamento per l’utilizzo di software utili ad implementare alcuni possibili rimedi;
- rilevazione “a posteriori” su 3 item della percezione globale del complesso delle minacce digitali in termini di loro gravità (a 7 punti), probabilità (risposta aperta) e disponibilità al pagamento per neutralizzarle (risposta aperta).

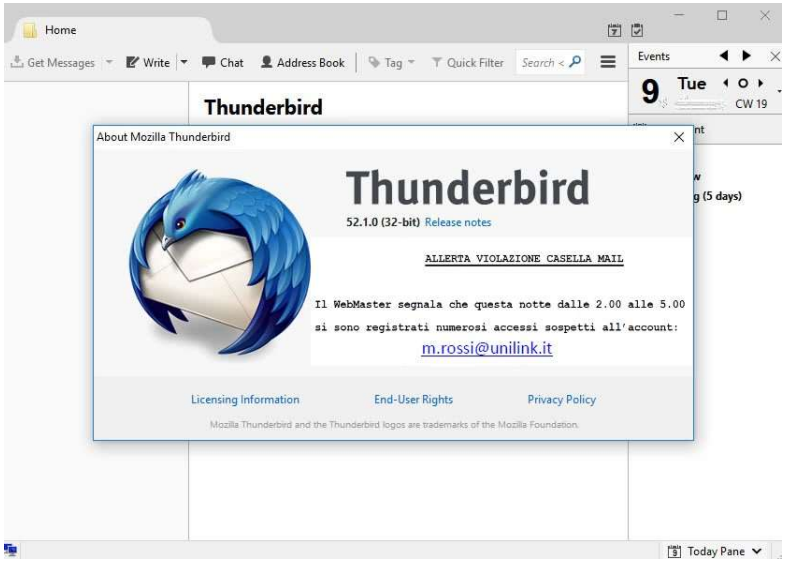
E’ possibile consultare ed anche affrontare il questionario attraverso il link https://goo.gl/forms/cnOx13BC5VlM8a093.

5.4 Manipolazione delle esperienze di abuso digitale

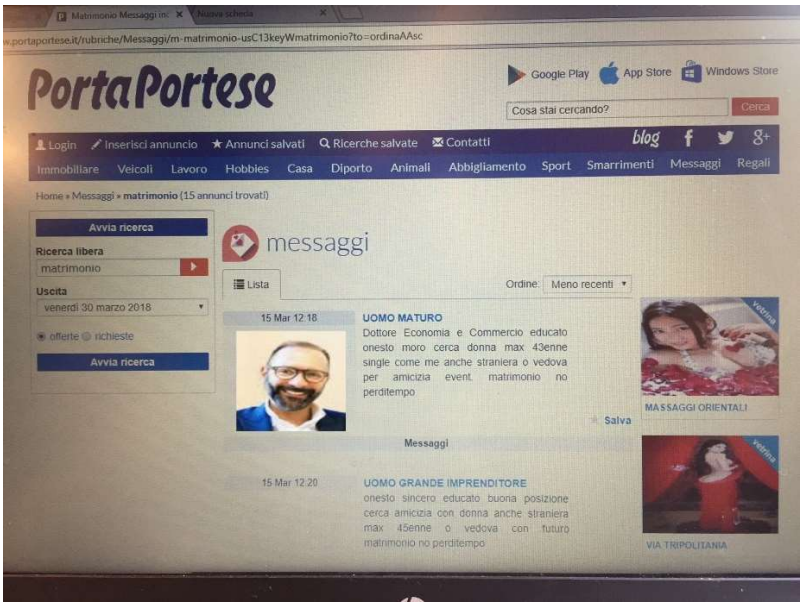
Il campione è stato casualmente suddiviso in due gruppi (24 e 25 partecipanti). Ad entrambi i gruppi è stata inviata una mail di allerta da parte di un amico collega con il seguente messaggio:

“Ciao, non so se lo hai già visto, ma ti invio con urgenza lo screenshot di un fattaccio che ti riguarda che ho appena visto on line. Penso che tu debba prendere pronti provvedimenti. Un abbraccio”.

Al primo gruppo (abuso prevalentemente “funzionale”) era quindi allegato uno screenshot rappresentante un messaggio di allerta per la violazione della propria casella mail istituzionale della Unilink.



Al secondo gruppo (abuso prevalentemente “espressivo”) era invece allegato lo screenshot di un sito di annunci matrimoniali in cui veniva illecitamente usata una foto personale del partecipante.



Ai partecipanti veniva chiesto di immedesimarsi nello scenario ipotetico rappresentato dalla mail e quindi di rispondere al questionario.

5.5 Risultati

L'esposizione dei risultati è organizzata secondo i cinque cluster di obiettivi sopra descritti.

Percezione delle specifiche minacce digitali

Per quanto riguarda la gravità delle 15 minacce, quella percepita più pesante è "cadere vittima del furto dei propri codici di accesso all'homebanking" (M = 6,35; DS = 0,83) seguita dalla "clonazione di bancomat o carte di credito" (M = 6,24; DS = 1,2), dal "furto di identità" (M = 6,00; DS = 1,15) e dal "furto di dati sensibili relativi ai propri familiari" (M =5,86; DS = 1,17). Sul versante opposto, le minacce percepite come meno gravi sono il "coinvolgimento in una "catena di Sant'Antonio"" (M = 3,45; DS = 1,99), venire "bombardato da spam" (M = 3,65; DS = 1,86) e "cadere vittima di "incidenti sociali" provocati dalla comparsa di inopportuni annunci pubblicitari di prodotti/servizi che lei ha precedentemente consultato (retargeting)" (M = 4,02; DS = 1,96).

Rispetto invece alle percezioni di probabilità di accadimento delle 15 minacce, quelle percepite più probabili nel corso della propria intera vita digitale sono la "aggressione da parte di un virus" dei propri dispositivi (M = 70,5%; DS = 27,5), il "bombardamento da spam" (M = 69,1 %; DS = 30,37) e il "coinvolgimento in una catena di Sant'Antonio" (M = 67,45%; DS = 35,71). Al contrario gli incidenti percepiti come meno probabili sono il "disconoscimento (ripudio) del proprio ordine di acquisto/pagamento da parte di un venditore online" (M = 48,06%; DS = 30,31), il "furto di identità" (M = 51,12%; DS = 30,1) e il "furto dei propri codici di accesso all'homebanking" (M = 53,4% ; DS = 24,65).

Combinando linearmente la probabilità e la gravità di ciascuna minaccia digitale emerge che le più pesanti sono la clonazione di bancomat e carte (M = 383,12; DS = 191), la aggressione dei virus (M = 379,47; DS = 183,41) ed il "cadere vittima di furto e uso improprio delle proprie immagini social" (M = 354,28; DS = 217,39). Al contrario gli abusi meno pesanti sono la catena di

Sant'Antonio (M = 242,34; DS = 206,39), il ripudio di un acquisto online (M = 245,51; DS = 190,34) e il retargeting durante la navigazione (M = 259,71; DS = 208,62).

Disponibilità al pagamento

Alla domanda relativa a quanto i partecipanti sarebbero disposti a pagare come premio di una polizza che li preservi nel corso della propria intera vita digitale da ciascuna delle 15 minacce, è emerso che gli incidenti per difendersi dai quali sarebbero disposti a pagare di più sono il furto dei propri codici di accesso all'homebanking (M = 125,86 euro; DS = 437,58), la clonazione delle proprie carte bancarie (M = 91,41 euro; DS = 189,34) e il furto di identità (M = 88,94 euro; DS = 206,31). Sul versante opposto, i partecipanti sono scarsamente propensi ad investire per proteggersi dallo spamming (M = 11,82 euro; DS = 34,89), dalle catene di Sant'Antonio (M = 16,41 euro; DS = 54,33) e da retargeting (M = 19,65 euro; DS = 76,98).

Percezioni globale del rischio digitale

Prima di analizzare le specifiche minacce i partecipanti assegnavano una gravità globale "a priori" pari a 5,29 (DS = 1,27) su 7 al complesso delle possibili minacce digitali, con una probabilità percepita del 66,61% (DS = 22,38) di loro occorrenza nel corso della propria intera vita digitale e con una disponibilità a pagare 89,94 euro (DS = 190,9) per difendersi.

Al termine della compilazione del questionario la percezione di gravità globale "a posteriori" risultava significativamente incrementata a 5,76 (DS = 1,21), $t(48) = -4,14$, $p < .0001$, mentre non risultavano significativamente diverse le percezioni di probabilità di accadimento (M = 60,82%; DS = 25,9) e la disponibilità al pagamento (M = 94,9 euro; DS = 195).

Infine, facendo la media delle percezioni di gravità, probabilità, e disponibilità al pagamento delle 15 minacce abbiamo potuto estrapolare una terza misura delle percezioni globali di rischio dei partecipanti.

In questo caso la gravità media percepita era pari a 5,17 (DS = 1,07) e non differiva significativamente dalle rilevazioni di gravità globale "a priori" e "a posteriori". Al contrario la probabilità media percepita era pari 59,03% (DS = 22,9) che era significativamente inferiore della valutazione "a priori" ($t(48) = 2,87$; $p < .01$) ma non differiva dalla valutazione "a posteriori". Infine, la disponibilità media al pagamento per difendersi dalle 15 minacce digitali è risultata pari a 59,85 euro (DS = 147,59) che era significativamente inferiore sia alla propensione globale "a priori" ($t(48) = 2,53$; $p < .05$) che a quella "a posteriori" ($t(48) = 2,97$; $p < .01$).

Risposte emozionali all'abuso digitale

Abbiamo chiesto ai partecipanti di valutare su una scala a 7 punti l'intensità delle seguenti reazioni emozionali in risposta alla visione dell'allegato rappresentante l'abuso da loro subito: rabbia, vergogna, ansia, imbarazzo, frustrazione, paura, delusione, impotenza e "senso di violazione". Abbiamo quindi confrontato attraverso un T test per campioni indipendenti le reazioni all'abuso "espressivo" (furto di immagini) rispetto a quello funzionale (accesso illecito alla mail professionale).

Le reazioni più intensamente sperimentate sono state il "senso di violazione" (M = 5,73; DS = 1,73), la rabbia (M = 5,43; DS = 1,37) e l'impotenza (M = 4,57; DS = 1,08). Al contrario quella più lieve è stata la delusione (M = 3,04; DS = 1,76), come se i partecipanti già non nutrissero elevate aspettative rispetto alla possibilità di essere preservati da abusi digitali.

L'abuso "espressivo" induceva reazioni emotive significativamente più intense rispetto a quello "funzionale", specificamente i partecipanti a fronte di un violazione delle proprie immagini esprimevano più intensamente rabbia ($t(47) = -2,71$; $p < .01$), vergogna ($t(47) = -4,99$; $p < .001$), ansia ($t(47) = -2,55$; $p < .05$), imbarazzo ($t(47) = -6,27$; $p < .001$) e senso di violazione ($t(47) = -2.09$; $p < .05$). Al contrario i livelli di frustrazione, paura, impotenza e delusione non differivano nelle due condizioni.

Rispetto alle specifiche percezioni di gravità, probabilità e disponibilità al pagamento relative all'evento critico da loro sperimentato, i partecipanti valutavano significativamente più grave l'abuso espressivo rispetto a quello funzionale, $t(47) = - 2,96$; $p < .01$), mentre le percezioni di probabilità di accadimento e la disponibilità al pagamento per neutralizzare la minaccia non differivano nelle due condizioni.

Gli effetti dell'abuso sulle percezioni dei rischi digitali

La tipologia di abuso che i partecipanti sperimentavano pareva non influenzare né le loro valutazione globali "a priori" del complesso dei rischi digitali né la loro disponibilità a pagare per una copertura complessiva, al contrario apparivano tendenzialmente influenzate le percezioni di gravità globale dei rischi digitali. Specificamente, chi aveva subito un abuso "espressivo" valutava i rischi digitali globalmente più gravi (M = 5,6; DS = 1,15) rispetto a chi aveva subito un abuso "funzionale" (M = 4,96; DS = 1,33), $t(47) = -1,8$; $p = .078$.

Tale influenza, come se sedimentasse nel corso della compilazione del questionario, appariva ancora più accentuata, raggiungendo la piena significatività, nelle valutazioni globali "a posteriori". In questo caso chi aveva subito un abuso "espressivo" valutava il complesso delle minacce digitali nettamente più grave (M = 6,2; DS = 0,91) rispetto a chi aveva subito un abuso "funzionale" (M = 5,29; DS = 1,33), $t(47) = -2,79$, $p < .01$.

Al contrario, e apparentemente paradossalmente, per la disponibilità "a posteriori" al pagamento di un polizza difensiva globale, emergeva che solo coloro che avevano subito un abuso "funzionale" erano disposti a pagare significativamente di più: 145,21 euro (DS = 241,99) contro 44,58 euro (DS = 117,72). Risultato che, nonostante sembri in contraddizione con le valutazioni di gravità, pare essere coerente con l'attitudine a valutare l'abuso "funzionale" più in termini economico-materiali e l'abuso "espressivo" più in termini affettivo-psicosociali.

Abbiamo anche analiticamente osservato come l'esperienza di abuso possa aver modificato le percezioni delle 15 specifiche minacce digitali.

Tra i risultati più interessanti emerge che l'abuso "espressivo" influenzava, incrementandola da 5,08 (DS= 1,53) a 6,16 (DS = 0,89) pure la percezione della gravità della violazione della propria posta elettronica, $t(47) = -2,98$; $p < .01$, rispetto all'abuso "funzionale" che era rappresentato proprio tale violazione. Inoltre l'abuso "espressivo" amplificava la percezione della gravità della minaccia del "furto dei propri codici di accesso ai social media" ($t(47) = -3,33$; $p < .01$), della minaccia di "furto di dati sensibili relativi ai propri familiari" ($t(47) = -2,43$; $p < .05$),

nonché sia la probabilità ($t(47) = -2,93$; $p < .05$) che la gravità ($t(47) = -3,61$; $p < .01$) di "furto e uso improprio delle proprie immagini social".

Atteggiamenti verso i possibili "rimedi"

Sulla base degli elementi emersi durante il focus group preliminare sono state formulate sei possibili misure utili a mitigare la probabilità e la gravità delle minacce digitali. Si è quindi invitato i partecipanti ad esprimere il proprio livello di accordo (su una scala likert a 7 punti) con ciascuna delle seguenti affermazioni rappresentative delle diverse contromisure.

a) "Per proteggersi sarebbe sufficiente che ogni utente fosse più attento e responsabile nel gestire la propria vita digitale"
b) "I siti dovrebbero fornire più informazioni quando chiedono all'utente autorizzazioni per l'accesso ai suoi dati"
c) "I siti dovrebbero evitare che l'utente dia l'autorizzazione in modo automatico e sovrappensiero"
d) "Gli strumenti di navigazione dovrebbero prevedere una funzione immediata e facile da attivare per la cancellazione di tutti i cookies in memoria"
e) "Gli utenti dovrebbero utilizzare una applicazione che li aiuti a gestire e aggiornare costantemente le proprie password"
f) "Gli utenti dovrebbero utilizzare una applicazione capace di setacciare il web e scoprire se una qualsiasi delle proprie immagini sia usata da qualcuno in modo improprio"

Il "rimedio" che più convinceva i partecipanti ($M = 5,9$; $DS = 1,65$) era il c) ovverosia il contrasto agli automatismi autorizzativi che spesso caratterizza la navigazione sul web. Al contrario la soluzione meno convincente appariva la a) ($M = 5,14$; $DS = 1,59$) indicando un orientamento dei partecipanti poco propenso a farsi personalmente carico dei propri comportamenti talvolta disattenti e superficiali nella gestione della propria vita digitale.

E' stata quindi posta ai partecipanti anche una domanda aperta volta a rilevare possibili suggerimenti su come concretizzare l'obiettivo sotteso al punto c), ovverosia che strategie dovrebbero implementare i siti per stimolare la consapevolezza degli utenti. Solo 7 partecipanti su 49 si sono avventurati a proporre delle soluzioni che spaziavano dall'invito a formulare messaggi brevi e chiari evitando il sovraccarico informativo, al vincolare l'utente alla lettura mantenendo la finestra di autorizzazione bloccata per almeno 30 secondi, all'usare warning sign o persino sms sul cellulare, all'astenersi dal chiedere ulteriori informazioni all'utente se già reperibili da altre fonti, fino al sarcastico invito ad utilizzare foto di nudo o di gattini (ovviamente in base all'appartenenza di genere) per catturare l'attenzione dell'utente prima di chiederne l'autorizzazione.

Infine, dal momento che tra i possibili rimedi figuravano l'utilizzo di due possibili applicazioni, è stato chiesto ai partecipanti di stimare il prezzo che sarebbero disposti a pagare per ottenerle. Per una applicazione che li supporti nel gestire e tenere aggiornate le proprie password i partecipanti si dischiaravano disposti a pagare 11,52 euro ($DS = 26,82$) mentre per una applicazione utile a cercare le proprie immagini sul web al fine di smascherare possibili abusi, i partecipanti erano propensi a pagare 28,52 euro ($DS = 67,46$).

La propensione ad utilizzare queste due applicazioni, ma non il prezzo che si era disposti a sborsare per ottenerle, era tendenzialmente influenzata dalle esperienze di abuso a cui i partecipanti erano stati sottoposti. Specificamente, la desiderabilità sia della app per la gestione

delle password che di quella per la ricerca delle immagini sul web veniva amplificata dall'esperienza di un abuso "espressivo" (rispettivamente, M = 5,68; DS = 1,7 e M = 6,04; DS = 1,24) rispetto a quella di un abuso "funzionale" (rispettivamente, M = 5; DS = 1,58 e M = 5,29; DS = 1,94).

6. Discussione

Analizzando comparativamente i risultati qualitativi del focus group con quelli quantitativi del questionario possiamo sviluppare una serie di riflessioni utili a comprendere in modo più accurato ed approfondito le rappresentazioni ed i fenomeni associati alla sicurezza digitale.

Innanzitutto emerge una congruenza tra le due rilevazioni. In entrambe la riflessione dettagliata sulle singole diverse minacce digitali che potenzialmente possono costellare e minare la sicurezza della propria vita digitale, porta ad un significativo incremento della percezione globale di rischio associato alle tecnologie digitali. In particolare nel focus group, probabilmente anche a causa della suggestività delle narrazioni prodotte dal gruppo in riferimento alle diverse tipologie di minaccia digitale, i partecipanti raddoppiano la propria disponibilità a spendere per una polizza a copertura dai rischi digitali al termine della sessione rispetto all'inizio. Pare in questo caso intervenire un classico effetto di "disponibilità" per cui gli individui tendono a valutare la gravità e la probabilità dei fenomeni sulla base della salienza emozionale delle loro espressioni più eclatanti e memorabili, salienza che pare essere galvanizzata dal confronto di gruppo.

Una interessante incoerenza tra le due rilevazione riguarda invece le percezioni delle singole minacce più gravi. Nel caso del focus group troviamo tra quelle più inquietanti il furto di identità e di documenti ed immagini relativi alla propria vita familiare e sociale, mentre il gruppo attribuisce solo una gravità media al furto dei codici homebanking e alla clonazione delle proprie carte di pagamento. Al contrario dal survey emerge che le minacce percepite più gravi sono proprio il furto dei codici homebanking e la clonazione delle carte, mentre il furto di immagini social e di identità è percepito di gravità più moderata.

In sostanza si assiste ad un rovesciamento dei pesi associati alle categorie di minacce che abbiamo distinto tra quelle determinanti un danno identitario/emotivo/psicosociale e quelle determinanti un danno operativo/economico/funzionale. Le prime appaiono più pesanti nella rilevazione qualitativa di gruppo mentre le seconde in quella quantitativa individuale.

Il fenomeno si può qui spiegare come un effetto "coerenza" indotto dal "response mode" più o meno sociale dei partecipanti. In sostanza un contesto gruppale finisce per rendere più pesanti le valutazioni di tipo psicosociale e simbolico mentre quello individuale fa prevalere le considerazioni di tipo materiale/"contabile"/cinico.

A fronte di questa incongruenza diventa interessante interrogarsi se sia più affidabile e 'realistica' una valutazione condizionata dal contesto sociale, come nel nostro focus, o una più individuale ed asettica come quella del nostro survey. In base alla teoria della identità sociale ipotizziamo che paradossalmente entrambe le valutazioni siano corrette in base a quanto prevalgano o meno, in un dato momento, le considerazioni sociali dell'utente. A questa paradossale "doppia sensibilità" possiamo attribuire quei fenomeni, talvolta drammatici, per cui un individuo può singolarmente decidere di compiere azioni digitali sconsiderate (come pubblicare materiale sensibile o offensivo sul web) per poi pentirsene sinceramente quando il suo "assetto" mentale tende a ritornare più sociale, ad esempio quando si confronta con amici rispetto alla opportunità della sua condotta digitale. Possiamo riconoscere in questa rappresentazione il fenomeno degli "haters" che nel vile isolamento davanti alla loro tastiera arrivano ad esprimere pensieri ed emozioni che loro stessi spesso misconoscono una volta immersi nella ricchezza di un contesto sociale significativo.

Vi è infine però una congruenza illuminante tra le nostre due rilevazione. In entrambe le metodologie combinando le riflessioni sulle percezioni di probabilità con quelle sulle percezioni di gravità delle diverse minacce emerge una convergenza sul peso psicologico di una specifica minaccia: il cadere vittima di furto e uso improprio delle proprie immagini social.

La nostra manipolazione sperimentale dell'abuso digitale mette nettamente in evidenza come l'uso improprio di una propria immagine provochi emozioni intense di rabbia, ansia, senso di violazione. Reazioni molto più marcate rispetto a quelle suscitate dalla violazione della propria casella mail professionale, nonostante questa minaccia fosse già percepita come una esperienza così pesante da spingere un partecipante al focus ad affermare "avrei in quel momento pagato qualsiasi cifra per rientrare e recuperare i miei documenti".

L'evidenza quantitativa del primato emozionale negativo dell'abuso relativo alle proprie immagini è coerente con le evidenze narrative del focus group che raccontano, ad esempio, dell'amica traumatizzata nel vedere le foto più care del proprio matrimonio utilizzate a sua insaputa a fini commerciali e promozionali.

I nostri dati dimostrano che essere esposti ad un abuso digitale associato all'uso improprio delle proprie immagini non solo provoca una reazione emotiva più vivida ma riesce ad influenzare globalmente, a causa di un effetto "prime", la percezione generale di rischiosità del web e tale valutazione negativa tende persino a peggiorare, come se sedimentasse, con il passare del tempo (ne hanno risentito specialmente le valutazioni globali conclusive dei nostri partecipanti).

Ne deriva che se l'obiettivo fosse quello di sensibilizzare rispetto ad un atteggiamento troppo disinvolto rispetto alle minacce digitali, una strategia brutale ma efficace potrebbe essere quella di esporre gli individui, previa loro autorizzazione, ad una esperienza di abuso digitale basato sulla violazione delle proprie immagini social. Ovviamente, in termini di impatto psicologico, tra il momento dell'autorizzazione da parte del soggetto e quello dell'esposizione all'abuso dovrebbe trascorrere un tempo sufficiente (ad esempio un paio di settimane) a generare un "pedagogico" effetto sorpresa. Potremmo spingerci a immaginare come alcuni genitori di adolescenti potrebbero arrivare a commissionare una esperienza sensibilizzante di questo tipo per i loro figli al fine di renderli consapevoli della inopportunità di condividere abbondantemente ed acriticamente le loro foto personali sul web.

In termini di potenziale di sensibilizzazione appare controintuitivo ma emblematico il fatto che una esperienza di abuso delle proprie immagini arrivi ad influenzare anche le percezioni di gravità relative ad una violazione della propria posta elettronica, evento che rappresentava l'altro polo della nostra manipolazione sperimentale.

Possiamo concludere le nostre riflessioni evidenziando il potere euristico di un ultima apparente incongruenza.

Da un lato l'abuso espressivo è percepito quello tra i più gravi e, quando sperimentato, quello emotivamente più impattante e più sensibilizzante rispetto alla gravità della costellazione delle minacce digitali, dall'altro i nostri partecipanti dichiarano una limitata propensione ad investire del denaro per proteggersi da questo tipo di rischio. I partecipanti a cui abbiamo fatto sperimentare lo scenario di una violazione della propria posta elettronica, pur valutando l'evento meno grave dell'abuso delle immagini, erano disposti a pagare più del triplo per una polizza a protezione della mail piuttosto che per una a protezione delle proprie immagini.

La spiegazione di questo paradosso può essere suggerita dagli studi dell'economista comportale Dan Ariely sulla incompatibilità che spesso si registra tra valutazioni di tipo economico

e fenomeni sociali. Immaginiamo un automobilista che cerchi un passante disponibile ad aiutarlo a cambiare una gomma offrendo una banconota da dieci euro piuttosto che semplicemente chiedendo una mano, o immaginiamo un seduttore che cerchi di convincere la sua compagna di una serata a concedersi tendando di sedurla ricordandole l'investimento economico che ha fatto tra ristorante e teatro quella sera. Questi sono esempi di come i fenomeni socialmente rilevanti (in positivo ed in negativo) rischino di venire alterati e corrotti da valutazioni e considerazioni di tipo economico.

Ne deriva che, pur i nostri partecipanti dichiarandosi disponibili a spendere mediamente più di 28 euro per una applicazione che li consenta di setacciare il web a caccia di un uso non autorizzato delle proprie immagini sui social, un servizio di tutela e protezione della propria "dignità sociale digitale" potrebbe essere percepito tanto più prezioso quanto più offerto gratuitamente a coronamento dell'acquisto di altri servizi digitali o al fine di fidelizzare i clienti di un brand che voglia veicolare così valori di tutela, benessere emozionale e protezione/valorizzazione identitaria.

6.1 Indicazioni applicative e possibili sviluppi della ricerca

Dall'insieme dei dati raccolti e dalla comparazione tra quelli quantitativi e quelli qualitativi possiamo in sintesi evidenziare quattro indicazioni applicative con relative possibili direttrici di approfondimento di ricerca.

a) Sviluppare una applicazione per la scoperta di abusi relativi alle proprie immagini personali e familiari.

   Le percezioni soggettive associate al rischio di questo abuso sono tra le più pesanti e la nostra manipolazione sperimentale che simulava la concretizzazione di questa minaccia ha elicitato le risposte emozionali più intense. Ne deriva che, soprattutto se fosse offerta come prodotto "premium" all'interno di un più ampio pacchetto di tutela e protezione, una applicazione capace di confrontare tutte le immagini nei propri profili social con tutte quelle presenti sul web, ed in grado di dare un pronto feedback all'utente rispetto alla loro diffusione, potrebbe rappresentare un prodotto gradito e rassicurante rispetto a uno degli scenari più inquietanti relativi alla sicurezza digitale propria e della propria famiglia. Possiamo immaginare un valore percepito ancora più elevato di una tale applicazione per un genitore che si sia fatto prendere troppo la mano nel postare sui social le foto dei propri bimbi e che, magari sensibilizzato dai media rispetto a qualche notizia di cronaca sul fenomeno della pedopornografia, senta forte la preoccupazione di verificare se il materiale sensibile da lui pubblicato possa essere stato oggetto di abuso. Affidarsi a questa applicazione potrebbe prontamente rassicurarlo o, nel caso peggiore, dargli gli strumenti per denunciare prontamente inquietanti illeciti.

b) Prevenire e mitigare i comportamenti miopi e antisociali in rete rendendo saliente la propria identità sociale.
   L'analisi comparativa intermetodologica dei nostri dati suggerisce che la sensibilità dell'utente verso i fenomeni digitali "espressivi" (ad esempio la tutela della propria immagine, la qualità emotiva della propria vita digitale, la difesa della propria identità) sia stimolata dalla salienza della "presenza sociale" da egli sperimentata (come nel caso del nostro affiatato gruppo di discussione). Quando questo senso di appartenenza

sociale viene affievolito incrementa la sensibilità per i fenomeni "funzionali" (ad esempio la tutela del proprio patrimonio, la protezione dalle truffe, il timore di subire furti economici). Da queste osservazioni possiamo ipotizzare che per l'utente potrebbe essere utile, quando deve effettuare valutazioni importanti o deve affrontare delle decisioni delicate o dalle possibili ripercussioni sociali significative ma trascurate (come quella di pubblicare un contenuto particolarmente estremo o aggressivo sul web), essere aiutato a tenere presente le sue appartenenze sociali più significative al fine di maturare valutazioni e decisioni più sagge, moderate e lungimiranti.

Operativamente si potrebbe pensare ad una applicazione, o ad una funzione dei portali social, che preventivamente faccia esprimere l'utente su quali siano le tre persone che più stima, più ritiene equilibrate, solide e degne di ammirazione. Tale rilevazione potrebbe essere anche presentata sotto forma di gioco avendo accesso alle proprie amicizie più significative nei social e invitando, come quiz ludico, ad esprimere una valutazione di valore sociale dei propri conoscenti. In questo modo si possono ricavare tre profili che probabilmente l'utente non vuole deludere e davanti ai quali non vuole sfigurare.

Una volta definita questa specifica "configurazione socialmente significativa" per ciascun utente, si potrebbe chiederne la autorizzazione preventiva ad utilizzarla nei momenti in cui l'utente stesse rischiando una condotta digitale della quale potrebbe pentirsi, ad esempio quando si rilevasse attraverso filtri semantici che il contenuto del post che sta scrivendo è particolarmente aggressivo. In questi casi il classico e notorio quesito-tormentone di Facebook "A cosa stai pensando?" si trasformerebbe in un saggio warning "Cosa ne penserebbero?", associato ad un piccolo box contenente i tre volti dei modelli sociali significativi indicati dall'utente stesso.

c) Sensibilizzare le fasce a rischio rispetto alla minaccia degli abusi digitali.

La nostra manipolazione sperimentale di concretizzazione di una minaccia digitale, ed in particolare della minaccia relativa all'uso improprio delle proprie immagini personali, ha determinato una serie di emozioni negative ma anche un incremento generalizzato della percezione del rischio relativo ad un ampio gruppo di possibili minacce digitali anche non specificamente associate al furto di immagini.

Ne deriva che un tale "trattamento sperimentale", pur nella sua cruda durezza, potrebbe rappresentare un intervento utile a rendere più consapevoli rispetto al tema della sicurezza digitale delle fasce di utenza che potrebbero tendere ad una condotta troppa disinvolta ed ingenua in rete.

Una attitudine di sottovalutazione dei rischi potrebbe ad esempio caratterizzare gli utenti giovanissimi o gli adolescenti.

Un genitore, in un contesto offline protetto, ad esempio quando il figlio troppo spregiudicato online è a casa e le sue risposte emotive al web possono essere gestite dalla famiglia, potrebbe affidarsi ad un servizio "provocatore" che, in ottica preventiva, faccia sperimentare al ragazzo una esperienza di abuso delle immagini personali che egli troppo incautamente ha reso disponibili sul web.

Come nel protocollo della nostra manipolazione sperimentale questo servizio contatterebbe l'ingenuo giovane utente rappresentandogli un utilizzo improprio, minaccioso e lesivo della propria immagine, magari utilizzando una foto "discutibile" (ad esempio, il ragazzo mentre fa linguacce e gesti volgari) segnalata dal genitore committente e che il servizio potrebbe minacciare di pubblicare diffusamente corredata di etichette svalorizzanti (ad esempio, "Ecco lo Scemo del Villaggio").

Questo intervento shock, se ben gestito, potrebbe rappresentare un vaccino capace di incrementare la maturità digitale dell'utente a rischio.

d) Gestione della percezione del rischio di danni materiali.

La percezione del rischio di danni economici derivanti da minacce digitali che colpiscono il rapporto con la propria banca e le proprie transazioni economiche tende, sia nella rilevazione qualitativa che in quella quantitativa, ad essere tra le più pesanti. Quindi gli utenti paiono essere inquietati dai rischi patrimoniali derivanti dal loro comportamento digitale.

Questa ansia potrebbe riflettersi in una vischiosità nel gestire digitalmente le proprie transazione (come nell'e-commerce) o le proprie operazioni bancarie (come nell'homebanking).

Nonostante sia nel focus che nel survey alcuni partecipanti abbiano esplicitamente affermato di essere consapevoli che in caso di abusi sarebbero stati tutelati dalla assicurazione fornita dalla propria stessa banca, registriamo una propensione a pagare (per una polizza a tutti gli effetti ridondante) ben 125 euro per proteggersi dal rischio di attacco al proprio portale di homebanking e 91 euro per proteggersi dalla clonazione delle proprie carte di pagamento. Forse anche per un effetto di ancoraggio tra la prospettiva del danno economico e la stima del valore della polizza, questi due prezzi sono i due più alti che abbiamo rivelato tra le disponibilità al pagamento per proteggersi da tutte le minacce digitali indagate. In sintesi i partecipanti, nonostante il loro generale rapporto evoluto con il web, sono disposti a pagare le cifre più alte per una copertura non necessaria.

Da queste osservazioni potrebbe svilupparsi una riflessione sulla opportunità di rendere più consapevoli gli utenti rispetto alle protezioni assicurative offerte dal sistema bancario in caso di abuso digitale di tipo patrimoniale.

A tal fine un "prime" che si potrebbe suggerire è semplicemente un box da far comparire nei momenti più ansiogeni della transazione (ad esempio quando viene richiesto di inserire i dati della propria carta di credito) che fornisca il dato "mobile" complessivo dei risarcimenti assicurativi agli utenti digitali pagati dal sistema bancario negli ultimi 365 giorni in tutto il mondo.

Probabilmente l'utente si troverà di fronte ad una cifra dell'ordine delle centinaia di milioni di euro che lo rassicurerà attraverso un meccanismo di "riprova sociale" rispetto alla tutela garantita dal sistema.

Ovviamente un tale box, e l'aggiornamento dei suoi dati, dovrebbe essere gestito da una istituzione internazionale (che dovrebbe anche monitorarne e perseguirne gli abusi) per essere reso disponibile solo ai siti di e-commerce più affidabili, diventando così sostanzialmente anche una sorta di ulteriore "marchio qualità".

References

[1] K. Amoako-Gyampah, J.R. Meredith, Examining cumulative capabilities in a developing economy, International Journal of Operations & Production Management 27 (2007) 928–950.

[2] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: a review and recommended two-step approach, Psychological Bulletin 103 (1988) 411–423.

[3] W.A. Arrindell, J. van der Ende, An empirical test of the utility of the observations-tovariables ratio in factor and components analysis, Applied Psychological Measurement 9 (1985) 165–178.

[4] R.P. Bagozzi, Measurement in marketing research: basic principles of questionnaire design, in: R.P. Bagozzi (Ed.), Principles of Marketing Research, Basil Blackwell Ltd., Massachusetts, USA, 1994.

[5] R.P. Bagozzi, Representing and testing organizational theories: a holistic construal, Administrative Science Quarterly 27 (3) (1982) 459–489.

[6] R.P. Bagozzi, Y. Yi, On the evaluation of structural equation models, Journal of the Academy of Marketing Science 16 (1988) 74–94.

[7] A. Benlian, M. Koufaris, T. Hess, Service quality in software-as-a-service: developing the SaaS-Qual measure and examining its role in usage continuance, Journal of Management Information Systems 28 (3) (2011) 85–126.

[8] P.M. Bentler, D.G. Bonnet, Significance tests and goodness of fit in the analysis of covariance structures, Psychological Bulletin 88 (1980) 588–606.

[9] P. Berghmans, K. Van Roy, Information security risks in enabling e-government: the impact of IT vendors, Information Systems Management 28 (4) (2011) 284–293.

[10] A. Bhatnagar, S. Misra, H.R. Rao, On risk, convenience, and Internet shopping behavior, Communications of the ACM 43 (11) (2000) 98–105.

[11] L.D. Bodin, L.A. Gordon, M.P. Loeb, Evaluating information security investments using the analytic hierarchy process, Communications of the ACM 48 (2) (2005) 79–83.

[12] K.A. Bollen, Structural Equations with Latent Variables, John Wiley & Sons, New York, 1989.

[13] K.A. Bollen, R. Lennox, Conventional wisdom on measurement — a structural equation perspective, Psychological Bulletin 110 (2) (1991) 305–314.

[14] M. Bruhn, D. Georgi, K. Hadwich, Customer equity management as formative second-order construct, Journal of Business Research 61 (12) (2008) 1292–1301.

[15] L. Casaló, C. Flavián, M. Guinalíu, The role of security privacy, usability and reputation in the development of the online banking, Online Information Review 31 (5) (2007) 583–603.

[16] C. Cegielski, Toward an interdisciplinary information assurance curriculum: knowledge and skill sets required of information assurance professionals, Decision Sciences Journal of Innovative Education 6 (1) (2008) 29–49.

[17] H.H. Chang, S.W. Chen, Consumer perception of interface quality, security, and loyalty in electronic commerce, Information & Management 46 (7) (2009) 411–417.

[18] R.K. Chellappa, P.A. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logistics Information Management 15 (5) (2002) 358–368.

[19] T.C.E. Cheng, D.Y.C. Lam, A.C.L. Yeung, Adoption of Internet banking: an empirical study in Hong Kong, Decision Support Systems 42 (2006) 1558–1572.

[20] C.M.K. Cheung, M.K.O. Lee, Trust in Internet shopping: instrument development and validation through classical and modern approaches, Journal of Global Information Management 9 (3) (2001) 23–35.

[21] C.M.K. Cheung, M.K.O. Lee, Understanding consumer trust in Internet shopping: a multidisciplinary approach, Journal of the American Society for Information Science and Technology 57 (2006) 479–492.
[22] L.J. Cronbach, Coefficient alpha and the internal structure of tests, Psychometrika 16 (1951) 297–334.
[23] F.D. Davis, R.P. Bagozzi, P.R. Warshaw, User acceptance of computer technology: a comparison of two theoretical models, Management Science 35 (1989) 982–1003.
[24] A. Diamantopoulos, P. Riefler, K.P. Roth, Advancing formative measurement models, Journal of Business Research 61 (2008) 1203–1218.
[25] A. Diamantopoulos, H. Winklhofer, Index construction with formative indicators: an alternative to scale development, Journal of Marketing Research 37 (2001) 269–277.
[26] T.E. Dube, R.A. Raines, G.L. Peterson, K. Bauer, M.R. Grimaila, S.K. Rogers, Malware target recognition via static heuristics, Journal of Computer Security 31 (2012) 137–147.
[27] Z. Erlich, M. Zviran, Goals and practices in maintaining information systems security, International Journal of Information Security and Privacy 4 (3) (2010) 40–50.
[28] X. Fang, S. Chan, J. Brzezinski, S. Xu, Moderating effects of task type on wireless technology acceptance, Journal of Management Information Systems 22 (2005–2006) 123–157.
[29] C. Flavian, M. Guinaliu, Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site, Industrial Management & Data Systems 106 (2006) 601–620.
[30] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1981) 39–50.
[31] R. Freeze, R.L. Rachke, An assessment of formative and reflective constructs in IS research, ECIS Proceedings, 2007, p. 171, (paper).
[32] D. Gefen, E-commerce — the role of familiarity and trust, OMEGA 28 (6) (2000) 725–737.
[33] D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated model, MIS Quarterly 27 (2003) 51–90.
[34] L.A. Gordon, M.P. Loeb, L. Zhou, The impact of information security breaches: has there been a downward shift in costs? Journal of Computer Security 19 (1) (2011) 33–56.
[35] V.K. Gurbani, A. McGee, An early application of the Bell Labs Security framework to analyze vulnerabilities in the Internet telephony domain, Bell Labs Technical Journal 12 (3) (2007) 7–19.
[36] J.F. Hair Jr., W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Multivariate Data Analysis, 6th ed., Prentice Hall, Upper Saddle, 2006.
[37] Harris Interactive, Online Security and Privacy Study, http://www.whitehouse.gov/files/documents/cyber/National%20Cyber%20Security%20Alliance%20-%20Harris+Online+Security+and+Privacy+Study.pdf (Accessed 18 August 2012).
[38] Edward Hartono , Clyde W. Holsapple , Ki-Yoon Kim, Kwan-Sik Na, James T. Simpson (2014) Measuring perceived security in B2C electronic commerce website usage: A respecification and validation, Decsion Support Systems, 11, 21
[39] J.B. Heide, G. John, The role of dependence balancing in safeguarding transactionspecific assets in conventional channels, Journal of Marketing 56 (January) (1988) 20–35.
[40] D.L. Hoffman, T.P. Novak, M.A. Peralta, Information privacy in the marketspace: implications for the commercial uses of anonymity on the web, The Information Society 15 (2) (1999) 129–140.
[41] L.T. Hu, P.M. Bentler, Fit indices in covariance structure modeling: sensitivity to underparameterization model misspecification, Psychological Methods 3 (1998) 424–453.
[42] C.B. Jarvis, S.B. MacKenzie, P.M. Podsakoff, A critical review of construct indicators and measurement model misspecification in marketing and consumer research, Journal of Consumer Research 30 (2) (2003) 199–218.

[43] S. Jayachandran, S. Sharma, P. Kaufman, P. Raman, The role of relational information processes and technology use in customer relationship management, Journal of Marketing 69 (2005) 177–192.
[44] M. Keil, H.K. Lee, T. Deng, Understanding the most critical skills for managing IT projects: a Delphi study of IT project managers, Information Management 50 (7) (2013) 398–414.
[45] M.Y. Kiang, Q. Ye, Y. Hao, M. Chen, Y. Li, A service-oriented analysis of online product classification methods, Decision Support Systems 51 (1) (2011) 28–39.
[46] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.
[47] C. Kim, W. Tao, N. Shin, K.S. Kim, An empirical study of customers' perceptions of security and trust in e-payment systems, Electronic Commerce Research and Applications 9 (2010) 84–95.
[48] J.W. Lian, T.M. Lin, Effects of consumer characteristics on their acceptance of online shopping: comparisons among different product types, Computers in Human Behavior 24 (2008) 48–65.
[49] Z. Liao, W.K. Wong, The determinants of customer interactions with Internetenabled e-banking services, Working Paper No. 0701, Department of Economics, National University of Singapore, 2007.
[50] N. Lim, Consumers' perceived risk: sources versus consequences, Electronic Commerce Research and Applications 2 (2003) 216–228.
[51] L. Liu, C. Li, S.J. Karau, A measurement model of trust in Internet stores, 2nd International Conference on Electronic Business, 2002, Taipei, Taiwan.
[52] C.S. Lu, K.H. Lai, T.C.E. Cheng, Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping, European Journal of Operational Research 180 (2007) 845–867.
[53] W. McFadzean, J.N. Ezingeard, D. Birchall, Information assurance and corporate strategy: a Delphi study of choices, challenges, and developments for the future, Information Systems Management 28 (2) (2011) 102–129.
[54] V.L. Mitchell, Knowledge integration and information technology project performance, MIS Quarterly 30 (4) (2006) 919–939.
[55] A. Motro, A unified model for security and integrity in relational database, Journal of Computer Security 1 (1992) 189–213.
[56] T. Noordewier, G. John, J. Nevin, Performance outcomes of purchasing arrangements in industrial buyer–seller relationships, Journal of Marketing 54 (1990) 80–93.
[57] J.C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1978.
[58] A. O'Cass, T. Fenech, Web retailing adoption: exploring the nature of Internet users web retailing behavior, Journal of Retailing and Consumer Services 10 (2003) 81–94.
[59] Office of Fair Trading (OFT), Findings from consumer surveys on Internet shopping: a comparison of pre and post study consumer research, http://www.oft.gov.uk/shared_oft/reports/Evaluating-OFTs-work/oft1079.pdf (Accessed 18 August 2012).
[60] M. Parent, The 6th and biggest lie of all: lessons from a decade of e-tailing, Ivey Business Journal Online 71 (8) (2007) 1–7.
[61] S. Petter, D. Straub, A. Rai, Specifying formative constructs in information systems research, MIS Quarterly 31 (4) (2007) 623–656.
[62] P. Podsakoff, D. Organ, Self-reports in organizational research: problems and prospects, Journal of Management 12 (1986) 531–544.
[63] G. Ramani, V. Kumar, Interaction orientation and firm performance, Journal of Marketing 72 (2008) 27–45.

[64] S. Ransbotham, S. Mitra, J. Ramsey, Are markets for vulnerabilities effective? MIS Quarterly 36 (1) (2012) 43–64.
[65] J.C. Roca, J.J. García, J.J. de la Vega, The importance of perceived trust, security and privacy in online trading systems, Information Management & Computer Security 17 (2) (2009) 96–113.
[66] J.J. Ryan, D.J. Ryan, Proportional hazards in information security [electronic version], Risk Analysis: An International Journal 25 (2005) 141–149.
[67] W.D. Salisbury, R.A. Pearson, A.W. Pearson, D.W. Miller, Perceived security and World Wide Web purchase intention, Industrial Management & Data Systems 101 (2001) 165–176.
[68] G.P. Schneider, Electronic Commerce, 9th ed., Cengage Learning, 2010.
[69] R. Sethi, Z. Iqbal, Stage-gate controls, learning failure, and adverse effect on novel new products, Journal of Marketing 72 (2008) 118–134.
[70] D.H. Shin, Ubiquitous computing acceptance model: end user concern about security, privacy and risk, International Journal of Mobile Communications 8 (2) (2010) 169–186.
[71] J. Simpson, C. Paul, The combined effects of dependence and relationalism on the use of influence in marketing distribution systems, Marketing Letters 5 (2) (1994) 153–163.
[72] M.T. Siponen, H. Oinas-Kukkonen, A review of information security issues and respective research contributions, The Database for Advances in Information Systems 38 (2007) 60–80.
[73] J.B.E.M. Steenkamp, H.C.M. Van Trijp, The use of LISREL in validating marketing constructs, International Journal of Research in Marketing 8 (1991) 283–299.
[74] E. Swilley, Technology rejection: the case of the wallet phone, Journal of Consumer Marketing 27 (4) (2010) 304–312.
[75] G. Torkzadeh, J.C.J. Chang, G.W. Hansen, Identifying issues in customer relationship management at Merck — Medco, Decision Support Systems 42 (2) (2006) 1116–1130.
[76] T. Tsiakis, G. Sthephanides, The concept of security and trust in electronic payments, Journal of Computer Security 24 (2005) 10–15.
[77] A. Usoro, S. Shoyelu, M. Koufie, Task-technology fit and technology acceptance models applicability to e-tourism, Journal of Economic Development, Management, IT, Finance and Marketing 2 (1) (2010) 1–32.
[78] G. Vaidyanathan, S. Mautone, Security in dynamic web content management systems applications, Communications of the ACM 52 (12) (2009) 121–125.
[79] B. Vatanasombut, M. Igbaria, A.C. Stylianou, W. Rodgers, Information systems continuance intention of web-based applications customers: the case of online banking, Information & Management 45 (2008) 419–428.
[80] W.F. Velicer, J.L. Fava, Effects of variable and subject sampling on factor pattern recovery, Psychological Methods 3 (1998) 231–251.
[81] M.M. Yenisey, A.A. Ozok, G. Salvendy, Perceived security determinants in ecommerce among Turkish university students, Behaviour & Information Technology 24 (2005) 259–274.
[82] S. Yousafzai, J. Pallister, G. Foxhall, Multi-dimensional role of trust in Internet banking adoption, The Service Industries Journal 29 (5–6) (2009) 591–605