QUADERNI DELLA REDOPEN FACTORY

E LIBERACI DAL MALWARE

SPUNTI PER UNA EDUCAZIONE CIVICA DIGITALE: PRIVACY E SICUREZZA INFORMATICA

Introduzione di Luigi Garofalo

ReD OPEN FACTORY
A CENTER FOR RESPONSIBLE INNOVATION

CASSA RURALE DI LEDRO
CREDITO COOPERATIVO ITALIANO

Ledizioni

Quaderni della ReD OPEN FACTORY

E LIBERACI DAL MALWARE

SPUNTI
PER UNA EDUCAZIONE CIVICA DIGITALE:
PRIVACY E SICUREZZA INFORMATICA

Ledizioni

2022 Ledizioni LediPublishing
Via Boselli 10, 20136 Milano
http://www.ledizioni.it
e-mail: info@ledizioni.it

Prima edizione Ledizioni: marzo 2022

E liberaci dal malware. Spunti per una educazione civica digitale: privacy e sicurezza informatica

ISBN cartaceo 978-88-5526-663-5
In copertina: immagini tratte da https://it.freepik.com

Informazioni sul catalogo e sulle ristampe: www.ledizioni.it

Indice

Prefazione

Luigi Garofalo
direttore del quotidiano online 'Cybersecurity Italia'
www.cybersecitalia.it

La sicurezza informatica è finita, all'improvviso, in cima alle agende di governi e Stati, perché gli attuali cyber-attacchi possono avere ripercussioni sulla sicurezza nazionale dei Paesi e bloccare anche l'erogazione di servizi essenziali. In Italia alcuni attacchi informatici hanno messo KO, per alcune ore fino a diversi giorni, i server di una Regione, di alcuni Comuni, aziende, Asl ed ospedali creando gravi disagi a cittadini, dipendenti, consumatori e pazienti.

E quasi sempre, involontariamente, "la breccia nel muro" è un dipendente con una scarsa cultura della sicurezza informatica, che ha aperto, incautamente, un'email truffa contenente un link da cui si è installato il software malevolo.

Per liberarci dal malware la prima difesa è il fattore umano, ecco perché questo Quaderno è utile: contribuisce, in modo semplice ed efficace, a veicolare la consapevolezza della cybersecurity nei lavoratori (nel settore pubblico e privato), nei consumatori, negli studenti (piccoli e grandi) e nei cittadini in generale.

Abbiamo tutti bisogno di una formazione base per saper riconoscere ed evitare i pericoli del web e, al tempo stesso, beneficiare dei vantaggi del vivere onli-

ne. In tutte le scuole andrebbe insegnata l'educazione civica digitale e questa iniziativa editoriale rappresenta uno dei validi *vademecum* da adottare.

Non esiste sicurezza informatica senza protezione dei dati e viceversa. Solo la cybersecurity, la data protection, la diffusione di un uso responsabile, da parte di genitori e figli, di device e social network e la condivisione di valori etici rendono il mondo digitale, anche nel metaverso, un posto bello da vivere e al sicuro da malintenzionati, da predatori di dati e dai cyber-criminali.

A livello di sistema Paese per rafforzare la cyber resilienza delle infrastrutture critiche dell'Italia è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN), che deve essere vista come i pompieri o la protezione civile degli incidenti cyber: interviene per rispondere al cyber-attacco e per mitigare gli eventuali impatti negativi. L'ACN man mano sarà composto da un corposo numero di cyberdefender: iniziamo a coltivare giovani agenti italiani della cybersecurity!

Guida alla lettura

Questo Quaderno è un contributo sul tema dell'educazione civica digitale e in particolare sulla tematica della protezione e prevenzione dalle più diffuse minacce informatiche che si possono incontrare usando smartphone, navigando in Rete e utilizzando piattaforme digitali.

Si parte dalla **Sicurezza informatica e la nostra quotidianità**, dando rilevanza a come alcune attenzioni che abbiamo nel vivere quotidiano siano utili e fondamentali anche nelle nostre attività e interazioni digitali. Questo ci porterà a capire che alla base della sicurezza c'è il sapere cosa rende sicuri noi e le nostre azioni, e perché.

Per capire a chi diamo i nostri dati, perché li concediamo e come possiamo proteggerli meglio, è utile la lettura dei "**Principi del GDPR**".

Ed eccoci passare ad una **Introduzione alla cyberd security**, a cui segue una lettura dedicata alle **minacce digitali** e ai **moderni cavalli di Troia virtuali**, sino ad arrivare a situazioni in cui si può essere **ricattati: i rana somware**.

Possiamo poi trovarci in situazioni di **Furto con destrezza, e…. senza contatto**, oppure correre il rischio di **essere pescati nell'oceano digitale**, pur essendo magari a casa in **Smart working**.

E per firmare con sicurezza un documento, **Firma elettronica e PEC** ci vengono in aiuto: rendere sicuri i documenti e le comunicazioni non è una missione impossibile.

In questo panorama abbiamo anche un tema di **Cyberbullismo** su cui agire.

Concludiamo infine questo percorso di educazione civica con alcune indicazioni su **come sopravvivere nell'era digitale**.

Chi vorrà continuare il percorso e approfondire uno o più temi, troverà in chiusura del quaderno i riferimenti istituzionali.

A CHI SI RIVOLGE?

Il quaderno tratta molti argomenti che riguardano la sicurezza informatica, cercando di farlo in tono divulgativo. Si rivolge così a chiunque sia abituato, vuoi per ragioni professionali vuoi per svago e intrattenimento, a svolgere attività in Rete, esponendosi a rischi e minacce informatiche.

PRIMA DI INIZIARE LA LETTURA

Liberarci dal *malware*, termine che indica software malevolo o virus informatico, è un'azione che spetta a noi avviare, un'azione dunque volontaria e consapevole.

La sfida oggi è quella di trovare un equilibrio tra un mondo di contatti e attività sempre più virtuali e il nostro vivere quotidiano con le sue relazioni di vicinanza. Acquisire consapevolezza permette di vivere la trasformazione digitale in atto con responsabilità verso di noi e soprattutto verso gli altri.

Del resto, quanto tempo abbiamo dedicato ad insegnare la pericolosità di forbici e coltelli? Per vivere consapevolmente la trasformazione digitale in atto, i

suoi rischi, benefici, vantaggi e pericoli serve molto meno tempo, e questo libro vuol essere un contributo in quella direzione.

Introduzione

Chiudere la porta di una stanza per la propria riservatezza o la porta di casa per sicurezza, essere certi di consegnare le nostri chiavi di casa a persone fidate, evitare luoghi pericolosi, non dare in mano forbici e coltelli a chi non è consapevole del potenziale pericolo: questi e altri comportamenti oggi vanno traslati anche negli spazi virtuali in cui ormai si svolge parte della nostra vita e in cui spesso lasciamo aperti altri tipi di porte. Per la tutela del nostro benessere e della nostra privacy, nello stesso modo in cui chiudiamo le porte fisiche, dobbiamo iniziare a considerare di chiudere – o gestire – le porte virtuali.

Social network, smartphone che dialogano con altri dispositivi che ci circondano, auto che guidiamo, riunioni online, lavoro a domicilio, oggetti "smart" presenti nelle nostre case o che indossiamo: queste e molte altre situazioni che viviamo quotidianamente ci obbligano ad essere consapevoli della *sicurezza informatica*, un tema che tempo fa era solo per addetti ai lavori.

Nella vita quotidiana decidiamo di dare fiducia al prossimo con cautela e diffidenza (a volte esagerando), però quando interagiamo tramite strumenti tecnologici, chissà come mai la nostra predisposizione alla fiducia verso gli sconosciuti aumenta a dismisura, la soglia di riservatezza cala ed ecco che condividiamo ciò che in un bar, ristorante, una pubblica piazza o altro luogo mai avremmo riferito a estranei.

Sicurezza e riservatezza ora hanno la necessità di essere declinate secondo altre regole; i nuovi oggetti tecnologici, infatti, ci pongono davanti a rischi che dobbiamo saper valutare e cogliere per poterli appunto evitare.

La fiducia è elemento fondante delle interazioni e dare fiducia nel mondo digitale è un atto molto semplice: basta un click! Per questo una maggior consapevolezza è d'obbligo: "fidarsi è bene, non fidarsi è meglio" oggi diventa il monito da tener presente anche in campo informatico.

Il pericolo esiste ed è per questo che dobbiamo impegnarci al massimo affinché la cybersecurity – sicurezza nel mondo digitale – e il concetto di privacy – riservatezza – si trasformino in qualcosa di tangibile, facilmente comprensibile a tutti, al di là di consensi dati sulla fiducia verso un'azienda, una persona o una organizzazione.

Questo è l'impegno che la **Cassa Rurale di Ledro, Banca di Credito Cooperativo**, ha attuato anche supportando e co-finanziando la pubblicazione di questa guida. L'iniziativa è un punto di partenza utile per stimolare la nostra individuale consapevolezza sulla responsabilità verso noi stessi e verso gli altri quando usiamo ciò che la tecnica informatica mette a disposizione di tutti noi.

Buona Lettura!

Lo staff di Red Open
Spin-off partecipato
Università degli Studi Milano Bicocca

Progetto sviluppo territoriale ledrense
della Cassa Rurale di Ledro: al servizio del territorio

La Cassa Rurale di Ledro B.C.C. rappresenta oggi il punto più alto dell'evoluzione del Credito Cooperativo di valle iniziato più di un secolo fa. Fa parte del Gruppo Cassa Centrale e conta attualmente su 4 filiali: Bezzecca, Molina, Tiarno di Sopra e Riva del Garda.

"*Fiducia reciproca, interesse comune*" è il messaggio in cui è racchiusa la mission della Banca, per la quale essere banca della comunità significa in primo luogo farsi carico delle necessità del territorio e lavorare insieme per incidere concretamente nella vita delle persone.

La Cassa Rurale di Ledro ha sempre messo al centro il forte legame con la comunità e il territorio in cui opera, sia dal punto di vista economico che dal punto di vista sociale; con questo spirito la Cassa Rurale di Ledro ha inteso contribuire alla realizzazione di questa pubblicazione informativa sul tema attuale dell'educazione al digitale.

L'educazione digitale ha origine dal presupposto che oggi, ogni giorno, ciascuno di noi incontra, in ogni aspetto della sua vita quotidiana, innovazioni tecno-

logie digitali e strumenti di intelligenza artificiale che ci coinvolgono nel lavoro, nel tempo libero, nella vita famigliare, nei rapporti con la pubblica amministrazione, tanto per citarne alcuni.

La trasformazione digitale in continua accelerazione porta con sé molte opportunità ma anche profonde implicazioni sociali, culturali ed etiche, che possono influire positivamente sul nostro benessere psicofisico e sociale ma possono nascondere anche molti rischi.

La nostra Cassa Rurale di Ledro con questa pubblicazione si pone l'obiettivo di aiutare ognuno di noi ad approcciarsi alle trasformazioni e alle innovazioni digitali con consapevolezza, spirito critico e responsabilità.

Sono infatti entrati purtroppo nel glossario comune e citati sempre più spesso nei fatti di cronaca termini come phishing, cyberbullismo, body shaming, revenge porn e sextortion (reati ed estorsioni a sfondo sessuale), furto di identità, challenge pericolose.

Siamo consapevoli che l'educazione digitale è destinata a non finire mai e dovrà evolvere con l'evolversi della materia che la stessa tratta.

Questa pubblicazione vuole quindi essere una base di partenza e uno spunto di riflessione a tutela di tutti, in particolare di bambini e ragazzi, bersaglio facile e innocente di chi sempre più frequentemente usa la tecnologia e l'innovazione in modo criminale.

Per il Consiglio d'amministrazione
Il Presidente
Baruzzi arch. Marco

Capitolo 1 – La sicurezza informatica e la nostra quotidianità

Ho chiuso la porta di casa?

Una cosa è certa, se la lasciamo aperta degli intrusi potrebbero entrare.

Se volgiamo lo sguardo dal mondo reale a quello digitale della Rete, con i suoi oggetti e dispositivi che giornalmente usiamo, il nostro atteggiamento cambia. Il più delle volte, infatti, lasciamo aperte porte virtuali, abbandoniamo informazioni personali incustodite e neanche ci sfiora il pensiero di possibili intrusi pronti ad approfittare della nostra disattenzione.

La sempre più assidua frequentazione di spazi virtuali ci obbliga perciò ad alzare il livello di consapevolezza dei rischi che corriamo utilizzando i vari gadget tecnologici che ci accompagnano quotidianamente, rischi spesso nascosti dietro ai vantaggi e che riescono a sottrarsi agli occhi di sistemi di allarme che pensiamo di aver installato.

Certo, posso affidarmi a esperti di sicurezza informatica che per mestiere si occupano di installare "allarmi" per prevenire ed evitare accessi ai sistemi informativi da parte di persone non autorizzate, ma occorre anche sapere cosa chiedere e, soprattutto, valutare come viene garantita la riservatezza delle nostre informazioni.

Occorre essere consapevoli dei rischi digitali, il che è meno complicato di quanto possa sembrare in partenza, anche perché le truffe informatiche, il phishing,

le tecniche di ingegneria sociale sfruttano la nostra disattenzione, la nostra inconsapevolezza, la curiosità e il più delle volte la fiducia che viene carpita attraverso l'inganno.

In fondo non è nulla di nuovo, sono solo cambiati gli ambiti dove ciò accade (la Rete, appunto) e i modi e gli strumenti attraverso cui viene reso possibile: lo smartphone *in primis*, perché la distrazione e l'uso dell'arte dell'inganno sono sempre stati elementi usati per creare situazioni di rischio.

Ad esempio, quanto tempo si è dedicato per insegnare ai minori che coltelli e forbici sono strumenti pericolosi da maneggiare, illustrando loro i rischi che corrono quando li usano?

Quanto tempo invece abbiamo speso a comprendere ed imparare a riconoscere i pericoli e i rischi del mondo digitale?

La sicurezza informatica, perciò, parte dalla nostra consapevolezza di ciò che può succedere utilizzando strumenti digitali, applicazioni o semplicemente navigando in Rete.

Riuscire a riconoscere situazioni ove si cerca di carpire la nostra fiducia è più semplice di quanto pensiamo, bisogna solo porsi alcune domande: le risposte ci aiuteranno a prevedere e gestire pericoli e rischi.

I capitoli che seguono ci aiuteranno a riconoscere le situazioni di rischio informatico e a prevenirle.

La prevenzione inizia con lo sviluppo di una consapevolezza personale di ciò che sono le nostre informazioni riservate e confidenziali, di come gestirle e proteggerle e di ciò che si intende per privacy. Faremo

questo anche attraverso le parole e i princìpi del regolamento europeo che protegge le persone disciplinando il trattamento dei loro dati personali.

Siamo stati catapultati in un mondo nuovo popolato di oggetti digitali che tra loro parlano e raccontano molto di noi. In questa realtà, dove digitale e fisico si intersecano, siamo tutti apprendisti che devono interiorizzare nuove regole e adattare le proprie abitudini e comportamenti a scenari, anche di rischio, inediti.

Se avessimo una cassaforte in casa, lasceremmo in bella vista la combinazione su un post-it?
Perché allora scriviamo le nostre password su un foglio e le lasciamo disponibili a terzi che potrebbero usarle?
Già con il bancomat una delle prime raccomandazioni era di evitare di mettere il PIN insieme alla tessera, perché in caso di smarrimento, o furto, un terzo poteva usarlo; stesso avvertimento vale per le password che usiamo per accedere ad applicazioni o siti.
Lo sappiamo che l'inganno dell'*Odissea* si ripete ogni giorno? Sono passati secoli dallo stratagemma di Ulisse che grazie all'inganno architettato, il Cavallo di Troia, permise ai greci di conquistare la città. Ebbene, ai giorni nostri trucchi simili vengono studiati per entrare nei nostri conti bancari, ottenere da noi informazioni e conquistare la nostra fiducia per poi poterne approfittare causandoci danni. Nel gergo informatico non a caso si chiamano *trojan* quei codici malevoli che si installano a nostra insaputa sui vari dispositivi.

Capitolo 2 – La protezione dei dati personali: princìpi generali

La sicurezza informatica nasce principalmente dall'esigenza di proteggere i dati, soprattutto personali, conservati e trasmessi tramite dispositivi digitali connessi in Rete.

È considerata dato personale l'informazione, spesso ma non necessariamente digitalizzata, che identifica – o che rende identificabile – una persona e le sue interazioni con altri individui, oggetti e luoghi.

Dal maggio 2018 è in vigore un regolamento europeo che protegge le persone disciplinando il trattamento dei loro dati personali, il GDPR (dall'inglese, *General Data Protection Regulation*). Tutti, più o meno direttamente, abbiamo a che fare ogni giorno con questa legge: quando ci iscriviamo alla newsletter di un blog, quando acquistiamo un bene online, quando veniamo assunti per un nuovo lavoro.

Il GDPR non impedisce il trattamento dei dati personali, ma fa sì che esso avvenga nel rispetto dei requisiti e delle modalità elencati nei suoi 99 articoli e 173 considerando. Il primo articolo illustra già gli ampi spazi di manovra lasciati a chi tratta dati personali:

- Mette in evidenza che la legge protegge le persone e garantisce la libera circolazione dei dati: *"Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati."*

- Si concentra sul diritto alla protezione dei diritti e delle libertà degli individui: *"Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali."*
- Ribadisce in chiusura il ruolo della libera circolazione: *"La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."*

Tre cardini su cui si regge il GDPR, che regola anche i diritti degli interessati – i cittadini i cui dati sono trattati – e le modalità del trattamento stesso. Infatti tutti gli individui, a fronte di un trattamento dei loro dati personali, hanno dei diritti, quali ad esempio essere adeguatamente informati, opporsi ad esso, richiedere l'accesso, la rettifica e la cancellazione e revocare il consenso dato.

Il trattamento avviene tra più parti, e due sono quelle essenziali: il titolare – ossia la persona, azienda, organizzazione che sta trattando i dati personali – e l'interessato, cioè noi.

Quando consentiamo l'accesso ai nostri dati è come se stessimo consegnando le chiavi di casa nostra a qualcuno che potrebbe entrare in nostra assenza. Nel caso concreto di solito ci accertiamo che la persona sia affidabile (probabilmente sarà un parente o un vicino di casa) e sappiamo non solo a chi le abbiamo date e perché, ma anche che possiamo riprenderle quando vogliamo, o quando non ci fidiamo più, o quando non

è più necessario che l'altra persona le abbia. Nel mondo digitale ci sono alcuni princìpi che regolano questo meccanismo di fiducia tanto comune nel mondo fisico. Si tratta di sei princìpi generali che chi raccoglie, tratta o memorizza dati personali all'interno dell'Unione Europea deve rispettare, facilitandoci così il compito di capire a chi stiamo consegnando le chiavi; in altre parole, rendendo chiaro e palese a chi stiamo concedendo le informazioni che ci riguardano, cosa stiamo firmando, a cosa stiamo dando il nostro consenso.

- *Liceità, correttezza e trasparenza del trattamento per colui che concede i suoi dati*. È necessario assicurarsi che le attività di raccolta e uso dei dati personali degli utenti non infrangano la legge e che nulla sia nascosto agli interessati. Per fare ciò, gli interessati hanno a disposizione l'informativa sulla privacy, ossia il documento che spiega in maniera chiara, concisa e completa perché, come e per quanto tempo i loro dati saranno utilizzati. E da chi.
- *Limitazione della finalità del trattamento*. Chi dà i suoi dati personali deve sapere per quale scopo sono raccolti; dev'essere uno scopo preciso che va indicato in modo chiaro nell'informativa. Inoltre, i dati devono essere conservati solo per il tempo necessario a raggiungere la finalità per cui sono stati raccolti.
- *Minimizzazione dei dati*. Si raccolgono e trattano i dati strettamente necessari. I titolari possono elaborare solo i dati personali necessari al raggiungimento della finalità per la quale sono trattati.
- *Esattezza e aggiornamento*. L'accuratezza dei dati

personali è parte integrante della loro protezione: i dati devono essere sempre esatti e tempestivamente aggiornati. La cancellazione dei dati che risultino scorretti deve essere tempestiva.

- *Limitazione della conservazione*: i dati non possono essere conservati per sempre, ma solo per un tempo non superiore a quello necessario al raggiungimento dello scopo per il quale sono stati raccolti. Non appena la finalità del trattamento è stata raggiunta, i dati devono essere tempestivamente cancellati.
- *Integrità e riservatezza*: i dati devono essere custoditi al sicuro e non possono essere diffusi. Il titolare deve garantire la sicurezza dei dati personali oggetto del trattamento. Chi tratta i dati, infatti, deve essere in grado di dimostrare che il trattamento è, in ogni sua fase, legittimo, secondo il principio della *accountability*, o responsabilizzazione, del titolare.

Alla luce del GDPR, il trattamento dei dati personali è possibile se rispetta i suoi princìpi generali, dunque, in primo luogo, se sono comunicate in modo trasparente le sue finalità e caratteristiche, tra cui la durata del trattamento, la quantità e qualità dei dati trattati, il numero degli interessati. Queste informazioni sono contenute nell'informativa sulla privacy, che spetta a noi leggere per essere consapevoli di ciò che firmiamo, di ciò che concediamo a terzi e del perché, per quali scopi e per quali usi.

Leggere l'informativa sulla privacy o il testo di un consenso al trattamento spesso non è semplice perché il linguaggio che ci troviamo davanti non è facilmen-

te accessibile per i non addetti ai lavori. Sapere quali informazioni andare a cercare all'interno di questi documenti ci garantisce quindi di raggiungere un primo livello di sicurezza: se investiamo un po' di tempo per identificare coloro a cui concediamo i nostri dati e per comprendere la finalità per cui li tratteranno, già dopo una prima lettura daremo la nostra fiducia con maggiore consapevolezza.

Minori e consenso privacy

Cosa succede quando i dati personali riguardano un minore? È possibile per i bambini e i ragazzi esprimere in autonomia la propria volontà all'uso dei propri dati personali per una certa finalità o servizio? Detto nei termini della privacy, ci stiamo chiedendo se e quando il minore può dare il consenso al trattamento dei propri dati personali.

In alcuni casi il trattamento di dati personali non è necessario allo svolgimento di un determinato servizio, oppure è fatto in modo da dover richiedere espressamente alla persona di cui vengono trattati i dati il permesso ad utilizzarli. Questo permesso si chiama, appunto, consenso.

Secondo il GDPR, il consenso è valido a partire dai 16 anni, età che può essere abbassata fino ai 13 anni nei singoli ordinamenti nazionali. In Italia il consenso al trattamento dei dati personali può essere espresso solo dopo il compimento dei 14 anni. Fino ad allora, sarà necessario che il genitore dia il permesso al minore di esprimere il consenso.

L'invito per i più giovani è, quindi, quello di non

fornire mai alcun dato personale a siti o piattaforme social almeno fino al compimento dei 14 anni e, in ogni caso, prendere tutte le precauzioni necessarie per comprendere per quali altre finalità potrebbero essere utilizzati i dati forniti. Queste informazioni sono comunicate nelle informative privacy, quelle che appaiono prima di poter accedere ai servizi online. Sono documenti complessi e lunghi, e anche in questo caso il consiglio è di sottoporli ad un adulto prima di accettare le condizioni proposte.

La privacy delle immagini in rete

Chi naviga in Internet e frequenta i social network si sarà chiesto cosa succede alle sue immagini una volta diffuse online.

Sempre più spesso condividiamo e pubblichiamo in Rete i nostri ricordi immortalati su scatti digitali, senza sapere di chi sia poi la proprietà di queste foto, chi possa utilizzarle e riprodurle, o chi ne abbia il controllo oltre a noi. Sempre più spesso inoltre si sente parlare di copyright, che è il diritto che l'autore di una certa immagine ha di sfruttarla economicamente. Affinché l'immagine sia coperta da copyright questa deve essere nuova, creativa e originale. Deve veicolare una certa volontà di carattere "artistico" e quindi, anche se non esiste una legge che stabilisca in maniera inequivocabile i criteri da seguire, è probabile che la foto amatoriale di un bellissimo tramonto scattata dal nostro telefono e condivisa sul gruppo dei nostri amici non sarà coperta da copyright. In caso di dubbio a decidere in merito alla creatività dell'opera dovrà essere un giudice.

Dunque cosa accade alle immagini condivise sui social? Qualsiasi social network che abbia la funzione "condividi" permette di "ripostare" immagini di altre persone sulla propria bacheca. Se ricondivido il post di un amico sul mio feed Instagram o nelle storie l'immagine diventa mia? No, resta di proprietà del mio amico.

Infatti, quando pubblico una foto sui social è come se permettessi alla piattaforma (Instagram, Facebook, TikTok o simili) di avere una licenza per poterla utilizzare, distribuire e condividere, a patto che l'immagine continui ad essere legata al mio account. Tant'è che, nel meccanismo di condivisione, restano ben visibili (o comunque facilmente reperibili) i nomi degli autori originari del video o della foto.

Questo significa anche che, se qualcuno decidesse di scaricare una foto da un social network e iniziasse ad utilizzarla come se fosse sua senza inserire i crediti dell'autore in ogni luogo in cui la foto viene esibita, si troverà nella condizione di aver violato il diritto dell'autore, commettendo così un illecito.

Capitolo 3 – Introduzione alla cybersecurity

Il GDPR disciplina diritti e doveri delle parti coinvolte nel trattamento dei dati personali, siano essi un indirizzo email, le coordinate del nostro conto corrente oppure dati relativi al nostro stato di salute. Il suo obiettivo è proteggere le persone cui quei dati si riferiscono e, allo stesso tempo, garantire la libera circolazione dei dati nel territorio dell'Unione Europea. Questo, lo ripetiamo, vale in particolar modo quando ci si muove nel mondo digitale, la cui pericolosità è meno percepita dalle persone rispetto a quanto non avvenga per il mondo fisico.

Eppure, tutti i giorni sentiamo parlare di furti di identità online, di violazioni di account email tramite attacco alle credenziali di accesso, di usi illeciti di codici di carte di credito.

Proteggersi, e proteggere i dati personali propri e dei propri cari, richiede anche di adottare precise misure di sicurezza che prevengono i rischi e, se qualcosa dovesse andare per il verso sbagliato, ne mitigano gli effetti.

Parlando di misure di sicurezza entriamo nella sfera della sicurezza informatica e, nello specifico, della cybersicurezza, o *cybersecurity*, e cerchiamo di capire come salvaguardare la nostra vita digitale, in tutti gli ambiti, da quello lavorativo e sociale, pubblico e privato.

Se la sicurezza informatica si occupa in generale del-

la sicurezza delle informazioni in qualsiasi formato (ad esempio, un documento cartaceo o una foto), la *cybersecurity* si preoccupa di proteggere specificamente le informazioni e i dati in formato digitale. Informazioni e dati, dunque, che troviamo su *hardware* (i nostri pc), *software* (i programmi e le applicazioni che usiamo regolarmente), e che vengono trattate su sistemi tra loro connessi (la Rete).

Quali accortezze per contesti digitali in continua evoluzione?

Quando suonano alla porta di casa, apriamo solo dopo aver riconosciuto chi chiede di entrare: ci assicuriamo cioè che entri solo chi riteniamo degno della nostra fiducia. Come siamo attenti e riservati sulle nostre vicissitudini, proprietà o altro ancora, allo stesso modo possiamo esserlo nel mondo digitale e nell'uso dei dispositivi annessi, applicando princìpi e comportamenti simili.

I dispositivi digitali e le piattaforme online erogatrici di servizi pubblici e privati (pensiamo all'e-commerce, ai servizi bancari e ai social network) hanno una diffusione vastissima e richiedono precisamente il tipo di attenzione di cui stiamo parlando, rendendo necessaria altrettanta cautela anche in Rete.

Il concetto di riservatezza infatti non cambia, a cambiare sono i luoghi dove la esercitiamo: da fisici e riconoscibili (se sono al bar mai urlerò le mie coordinate bancarie), a luoghi dove potremmo non renderci conto di essere esposti ad un pubblico di sconosciuti, e finiamo con il dare quelle stesse notizie e informazio-

ni su di noi che non urleremmo ai quattro venti sulla pubblica piazza.

Che fare dunque, oltre a tenere in considerazione i princìpi generali della privacy?

Come prima azione, valutiamo sempre quanto è sicuro il luogo dove mettiamo le nostre informazioni e chi sono coloro a cui le affidiamo.

Il secondo passo è essere sicuri di avere le chiavi di quel luogo, ovvero le credenziali e le relative password, che gestiremo come già facciamo con le chiavi di casa o dell'auto: evitiamo di lasciarle in giro a disposizione di terzi.

Da piccoli ci è stato insegnato a usare forbici e coltelli senza farci male. Oggi, da adulti, dobbiamo sviluppare la stessa accortezza di fronte ai rischi digitali: maneggiamo ogni giorno qualcosa che può essere pericoloso per noi e per altri. L'uso sbagliato può infatti arrecare danni economici, di credibilità e di reputazione a noi e a terzi. Le informazioni condivise con leggerezza possono creare falle di sicurezza che attori malevoli sono pronti a sfruttare.

Tempo fa esisteva una guida per evitare i furti in casa, e forse dovrebbe tornare di moda, visti i casi eclatanti di personaggi famosi inebriati dal loro momento di celebrità che postano foto di attimi di festa sui vari social network per poi tornare a casa e trovarla svaligiata. Cos'era successo? Avevano detto a tutti che la loro casa era incustodita: anche a coloro che magari li hanno sorvegliati "digitalmente" per poter poi approfittare del momento giusto.

"Se non lo paghi, il prodotto sei tu"

Oltre ai pericoli in cui possiamo incorrere, soggetti terzi possono usare informazioni e dati che ci riguardano per arricchirsi: non toccano i nostri portafogli o risparmi, ma usano noi e quello che facciamo online come elemento produttivo delle loro piattaforme digitali.

Pensiamo al tracciamento "consensuale" dell'individuo che naviga in Rete (e ha accettato frettolosamente i famosi *cookie*, i "biscotti" digitali che memorizzano chi e quando è passato per un sito Internet), che siede al tavolo di un ristorante (e diffonde sui social dove si trova, cosa sta mangiando, e magari anche in compagnia di chi), che condivide stralci delle proprie giornate sui social network. Terzi sconosciuti trasformano tutto questo in prodotti, per esempio vendendo come ci comportiamo, le nostre preferenze e abitudini a chi fa pubblicità che quindi saprà con cosa spingerci al prossimo acquisto di cui non sapevamo neppure di avere necessità.

Minimizzare…gli errori umani

Educazione all'uso di nuovi strumenti, consapevolezza della loro utilità e pericolosità, presa di coscienza di ciò che autorizziamo con il nostro consenso, cura e mantenimento della riservatezza sono dunque i capisaldi di una vita digitale serena.

La *cybersecurity* ci aiuta a presidiare il nostro spazio e le azioni sulla Rete: protegge i sistemi e i nostri dati, impedisce che persone e organizzazioni non autorizzate possano accedervi e, insieme, consente l'accesso a

chi autorizziamo espressamente.

Le misure di sicurezza non si limitano alle strutture fisiche – l'hardware e il software dei sistemi di sicurezza – o alle procedure operative – di autenticazione e di accesso –, ma si estendono alle procedure di gestione del sistema, il personale e i sistemi di comunicazione.

L'errore umano è infatti la causa più probabile e più frequente degli incidenti informatici, anche dei nostri personali incidenti.

L'errore è talvolta indotto da terzi in maniera intenzionale: carpire la nostra fiducia attraverso l'inganno è storia vecchia sin dai tempi di Ulisse e del cavallo di Troia, e non a caso alcune tecniche di intrusione nei dispositivi digitali e di attacco ai sistemi informatici prendono il nome di *trojan*. Il *trojan* è un codice malevolo, o virus, che si insinua nel nostro sistema attraverso una applicazione che crediamo benevola. Installando l'applicazione, diamo il via all'installazione del virus.

Quando l'incidente di sicurezza informatica è intenzionale e malevolo, è un attacco, quando invece l'incidente è involontario, è un errore. Ma il fatto che sia un errore non evita il verificarsi di conseguenze dannose e non impedisce di pagare un costo anche elevato per ripristinare la situazione.

Sia che si tratti di attacchi sia che si tratti di errori, alzare le prime barriere di protezione tocca a noi, protagonisti della scena digitale attraverso l'uso assiduo dei social network, delle app, dei vari device (tablet, smartwatch, etc.) che ci agevolano durante la giornata.

Nei capitoli che seguono, abbiamo illustrato altri accorgimenti e conoscenze utili per diminuire le possi-

bilità che gli errori si verifichino e gli attacchi vadano a buon segno. Nel frattempo, mettiamo in pratica questi primi consigli generali e aumentiamo la consapevolezza di come vivere in Rete in sicurezza.

Capitolo 4 – Le minacce digitali

Oggigiorno, per svariati motivi, si è sempre più connessi ad Internet e pertanto ogni dispositivo collegato è potenzialmente esposto ai pericoli della Rete. I gruppi di cyber criminali sono in costante aumento e prendono di mira diversi target al fine di poterne trarre profitto. Il crimine informatico si organizza ormai con strategie di business e opera prevalentemente nel dark web, dove è possibile anonimamente acquistare malware e affittare servizi per attaccare reti casalinghe o aziendali.

Particolare interesse rivestono i dati dei clienti sottratti alle aziende sanitarie private o agli ospedali pubblici: nomi di persone, date di nascita, contatti e-mail, codici fiscali, numeri di carte di credito e, come spesso accade nei paesi anglosassoni, numeri di previdenza sociale e dati sanitari (malattie, interventi chirurgici, allergie). Un caso eclatante, avvenuto negli Stati Uniti nel 2017, è stato l'attacco subìto dall'agenzia di segnalazione crediti Equifax, alla quale sono stati sottratti i dati di quasi la metà della popolazione statunitense.

La sottrazione di dati personali può essere sfruttata dai malviventi in diversi modi: per esempio vendendo nel mercato nero questi dati che generalmente vengono utilizzati per compiere altre frodi o per campagne di spam, oppure ricattando le aziende a cui sono stati sottratti, richiedendo denaro in cambio di una non divulgazione dei dati stessi.

I **vettori di attacco**, cioè le vie usate per sferrarlo, possono essere molteplici: ad esempio può avvenire tramite **chiavette USB infette** che eseguono un codice nocivo quando vengono inserite nel computer, oppure tramite altri dispositivi USB come **mouse**, ventilatori, ecc., apparentemente innocui ma modificati *ad hoc* per colpire la vittima designata nel momento in cui il dispositivo viene collegato al pc del malcapitato.

L'attacco può essere sferrato anche tramite pagine web create appositamente per diffondere il contagio, sfruttando ad esempio un **bug**, ovvero un difetto o anomalia, che provoca il malfunzionamento di un software, del browser web o del sistema operativo. Ancora, l'infezione può avvenire tramite l'**apertura di documenti infetti** creati appositamente allo scopo, o tramite **e-mail di phishing** che possono contenere allegati o link ingannevoli, e di cui parleremo in modo approfondito più avanti.

Anche tramite l'**esecuzione di software pirata** scaricato da canali di dubbia provenienza è possibile contrarre l'infezione: questi software in apparenza funzionano per lo scopo per cui sono stati sviluppati, ma al loro interno includono anche codice malevolo che può compiere le più svariate azioni. Questo vale anche per smartphone e tablet: non accade così raramente, infatti, di incappare in app presenti anche nel Play Store di Google che contengono codice malevolo.

I controlli effettuati da Google sono infatti meno rigorosi di quelli eseguiti da Apple sulle applicazioni caricate sul proprio App Store, e l'utente ha quindi il compito di prestare ancora più attenzione a ciò che

scarica e installa sul proprio dispositivo. Ricordiamo il caso in cui un bug nel sistema automatico di verifica delle app nel Play Store di Google ha permesso a uno sviluppatore di caricare un'app denominata Update WhatsApp Messenger. L'app riportava come produttore il nome WhatsApp Inc., seguìto da alcuni caratteri "Unicode": quindi il produttore risultava essere WhatsApp Inc. con altre lettere che non erano però visualizzate dall'utente. Usando questo trucchetto, il sistema di controllo del Play Store identificava i due produttori come differenti e non rilevava alcuna anomalia.

Un altro vettore di infezione in aumento è il "malvertising" (parola composta da "malicious" e "advertising"): si tratta di pubblicità create con lo scopo di infettare chi clicca sull'annuncio o anche solo si connette alla pagina che le contiene; si trovano spesso nelle pagine che permettono di vedere in streaming opere coperte da copyright. Queste campagne di pubblicità ingannevole tentano di indurre il navigatore a scaricare e installare antivirus fasulli, ad effettuare aggiornamenti di plug-in del browser web come ad esempio Adobe Flash Player (tecnologia che si sconsiglia di utilizzare per via delle sue note vulnerabilità), Java o fasulli codec video che, a detta del messaggio pubblicitario, servirebbero a visualizzare correttamente i filmati in streaming. E questi sono solo i casi più famosi e frequenti: i produttori di malware si dimostrano molto fantasiosi quando si tratta di raggirare l'utente. Non sempre i siti che ospitano le pubblicità fasulle sono consapevoli della loro presenza, perché solitamente

per le campagne pubblicitarie si affidano a società terze che inviano sul sito del cliente i messaggi pubblicitari: sono loro a mettere in atto questi trucchetti per ingannare i visitatori.

I dispositivi presi di mira continuano a essere server, computer, dispositivi mobili quali cellulari o tablet, ma verranno sempre più colpiti anche dispositivi intelligenti di uso quotidiano: modem, router, telecamere di videosorveglianza e dispositivi IoT (Internet of Things), di uso sia domestico sia industriale, connessi a Internet, il cui numero sta aumentando in modo non indifferente, senza che ce ne rendiamo conto (pensiamo alla lavatrice collegata alla app per il suo funzionamento, oppure all'assistente vocale che ci aiuta ad accendere e spegnere l'illuminazione a casa). Ad esempio, il malware Mirai (e sue nuove varianti) colpisce i dispositivi IoT che, una volta infettati, possono essere utilizzati per mettere in atto attacchi verso altri obiettivi. Nello specifico, il malware Mirai metteva in atto un attacco DDoS (Distribuited Denial of Service) al fine di saturare le risorse dei server colpiti per metterli fuori uso. Potenzialmente, attacchi mirati a dispositivi di questo tipo possono far entrare l'aggressore dentro la Rete interna, permettendogli così di sferrare ulteriori attacchi.

Incursioni di questo tipo saranno sempre più frequenti perché gli IoT sono spesso progettati senza pensare alla sicurezza (ad esempio, sono configurati in modo non corretto e le credenziali d'accesso di default sono note o facilmente reperibili sui manuali di configurazione) e senza che l'utente finale neppure sospetti la presenza di falle aperte in dispositivi che usa quo-

tidianamente. In fondo, chi si aspetterebbe che il suo frigorifero intelligente o la sua lavatrice smart siano punti di accesso alla Rete domestica?

Se hai acquistato un assistente digitale (Smart Assiu stant) per la tua casa o utilizzi regolarmente quello messo a disposizione dal tuo smartphone, segui le accortezze indicate dal Garante privacy, l'Autorità italiana per la protezione dei dati personali:

1. Informati su come vengono trattati i tuoi dati, cioè leggi l'informativa sulla privacy, capisci chi tratta i tuoi dati personali, come e per quanto tempo.
2. Limita le cose che dici al tuo assistente digitale, ossia non dare informazioni non necessarie, ricordati che le tue parole, per qualche anomalia intenzionale o per errore, potrebbero essere ascoltate da terzi non autorizzati e malintenzionati.
3. Disattiva l'assistente digitale quando non lo usi, diversamente il dispositivo rimarrà in "ascolto passivo" per captare la parola di attivazione e non è facile sapere con certezza se i dati raccolti in questa fase (come suoni o immagini) sono conservati e/o condivisi con terze parti.
4. Decidi quali funzioni mantenere attive, soprattutto se in casa hai più assistenti digitali e li usi tutti insieme per funzioni domotiche, ossia per rendere la tua casa intelligente. Quest'uso presenta il rischio di trattamenti non previsti dei tuoi dati personali, attraverso scambi, incroci e diffusione delle informazioni. Valuta se inserire una password per l'attivazione di specifiche funzioni.

5. Cancella regolarmente la cronologia di quanto registrato dall'assistente digitale.
6. Metti la sicurezza al primo posto: ad esempio, scegli password di accesso complesse e cambiale periodicamente.
7. Cancella i tuoi dati e gli account collegati all'assistente digitale se decidi di venderlo o regalarlo. Se i dati sono stati trasmessi alla casa produttrice (verificalo leggendo l'informativa sulla privacy), puoi sempre chiederne la cancellazione. È un tuo diritto!

Fonte: https://tinyurl.com/mvtfe8ez

Capitolo 5 – L'Odissea digitale, i moderni cavalli di Troia

L'arte dell'inganno è antica come l'uomo, e oggigiorno emergono continuamente nuovi strumenti e nuove modalità per carpire la nostra fiducia ed ingannarci, inducendoci a fare ciò che forse non avremmo mai fatto. Ci occupiamo ora dei nuovi e moderni cavalli di Troia usati per indurci ad aprire le porte dei nostri dispositivi e far entrare coloro che sono intenzionati a procurarci qualche danno.

Nel capitolo 4 abbiamo introdotto i vettori di attacco, ossia la strada (chiavette USB, email di phishing, app malevole, etc.) scelta dall'hacker per colpire. Il vettore infatti ha il compito di introdurre all'interno del sistema il malware, cioè il software dannoso (malware viene da *malicious software*). Questi software dannosi possono essere classificati in tre macrocategorie:

1) **Trojan o Trojan horse**: il malware si nasconde all'interno di un programma, generalmente utile, che viene offerto all'utente o condiviso da altre persone. Può essere trasmesso tramite mail, scaricando file o programmi, all'interno dei quali il trojan rimane latente fino al momento della sua installazione. Il trojan, in generale, non è altro che uno strumento che consente ad altri tipi di infezioni informatiche di propagarsi nel dispositivo infettato, nonostante ne esistano anche diverse tipologie con funzioni specifiche, come il captatore informatico. Il trojan può essere considerato sia virus, sia vettore, poiché risulta essere un "lasciapassa-

re" per altri contenuti dannosi.

2) **I virus** veri e propri: sono programmi maligni che o si sostituiscono o si copiano all'interno di un altro programma, aspettano la sua esecuzione e al momento in cui avviene infettano il resto del sistema mentre il programma originale opera.

3) **I Worm**: la distinzione con i virus è dovuta al fatto che i frammenti di codice binario con cui sono scritti i worm sono autonomi, e agiscono per intaccare le memorie, consumare le risorse del sistema e propagarsi velocemente nei sistemi connessi. A differenza del trojan non sono tecnicamente dei parassiti, non necessitano infatti di essere collegati ad un programma per replicarsi, ma sfruttano la Rete sia locale sia di Internet, e pur non essendo estremamente minacciosi, se presi singolarmente, lo diventano nel momento in cui si propagano come un'epidemia, infettando più dispositivi possibile, e mettendo di conseguenza a rischio la sicurezza dei sistemi e delle reti.

4) **Man-in-the-Middle**: in questo attacco l'hacker si posiziona tra l'utente e il server che si vuole raggiungere. L'attaccante registra le informazioni che transitano tra il server e il client che li richiede, ma senza interrompere la trasmissione in modo che l'attaccato non si accorga di nulla. Quanto l'utente non è più attivo si possono vendere o utilizzare le informazioni o le credenziali raccolte.

Che cosa hanno in comune questi tipi di attacchi? Tutti inducono con l'inganno l'utente a trasmettere i propri dati o le informazioni riservate in luoghi e a persone a cui non dovrebbero essere trasmessi. Alcuni

di essi si possono prevenire tenendo sotto stretto controllo hardware e software. Per altri invece non è sufficiente avere sistemi che siano tecnicamente in ordine, perché l'hacking non è di tipo tecnico, ma **cognitivo**. Questo tipo di attacchi è quello che si sta diffondendo maggiormente e dà ottimi risultati perché le vittime sono, il più delle volte, semplici utenti dei sistemi. È quindi necessario fare in modo che gli utenti siano in grado di difendersi da attacchi di tipo cognitivo prendendo coscienza dei pericoli impliciti nell'uso delle tecnologie dell'informazione e della comunicazione (anche dette ICT).

Ad esempio, un malware derivato da Mirai (ne abbiamo parlato nel capitolo precedente, a proposito degli attacchi ai danni dei sistemi IoT), di nome Dubbed Satori, scoperto dalla società di sicurezza Check Point, ha preso come bersaglio uno specifico modello di router domestico, l'HG532 di Huawei. Sfruttando alcune vulnerabilità di quel modello, il malware faceva rispondere il router a comandi arbitrari e gli faceva caricare software dannosi, rendendolo una marionetta a disposizione del suo burattinaio. I dispositivi Huawei HG532 sono stati colpiti un po' in tutto il mondo, soprattutto negli Stati Uniti, in Germania, in Egitto e anche in Italia. Varianti di Dubbed Satori sono in continua evoluzione e colpiscono dispositivi di varia natura, espandendo ulteriormente la lista dei vulnerabili: un gruppo di ricercatori cinesi ha scoperto una variante che infetta i computer che fanno mining delle criptovalute, sostituendo l'indirizzo del conto virtuale del cripto-minatore con quello del creatore del malware.

La maggior parte delle volte questi tipi di attacchi sono del tutto invisibili all'utente che, in particolar modo in ambito domestico, non ha gli strumenti per rilevare (o anche solo sospettare) le anomalie nella sua Rete. Ma non è solo il privato ad essere minacciato: anche i dispositivi di controllo industriale, ossia quelli che dirigono la produzione nelle raffinerie e negli altiforni, sono soggetti a potenziali attacchi che mettono a rischio non solo i dati, ma l'incolumità degli operatori e delle persone che vivono nei pressi dei centri di produzione.

Per evitare questo genere di problemi è opportuno cambiare le credenziali di accesso di default e mantenere il firmware, ossia il software interno al dispositivo, sempre aggiornato. A causa dell'obsolescenza del dispositivo, però, non sempre sono disponibili gli aggiornamenti del firmware, perché il produttore smette di seguire il device che ha prodotto. In questo caso, l'alternativa è quella di acquistare un dispositivo più recente, che presumibilmente avrà un firmware più aggiornato e un supporto per gli aggiornamenti più esteso. Più raramente, è possibile utilizzare i firmware sviluppati dalla comunità *open source*, ossia dai sostenitori del software libero da vincoli proprietari: si tratta però di un'operazione non praticabile per tutti i dispositivi, e che richiede competenze specifiche per la sua esecuzione. Si suggerisce, quindi, di aggiornare qualsiasi dispositivo interconnesso, dal modem alle telecamere di sorveglianza passando per le smart TV e, qualora il dispositivo non fosse più supportato dal produttore, si deve valutare se non sia il caso di acqui-

stare un nuovo dispositivo, anche se "funziona ancora tutto".

Anche per i computer vale la regola d'oro di **mantenere aggiornato** sia il **sistema operativo** (Windows, macOS o Linux) sia i **software installati**, come ad esempio il browser web ed i plugin, e di evitare di utilizzare componenti con una tecnologia obsoleta e vulnerabile, come ad esempio Adobe Flash Player. È inoltre necessario installare un **antivirus**, che deve essere aggiornato **quotidianamente**, e un firewall software, cioè un programma che evita gli attacchi dall'esterno e che controlla se qualche software cerca di collegarsi all'esterno in modo non autorizzato – per chi tratta dati personali di terzi, questa non è solo una necessità tecnica, ma anche un obbligo di legge. C'è poi da sfatare il mito che gli antivirus servano solo per i sistemi Windows: servono anche in ambiente macOS, perché macOS è un sistema ormai molto diffuso, e quindi viene preso di mira da virus, malware e crypto locker. E anche se si usa Linux, cioè un sistema operativo *open source*, è meglio pensare a programmi che proteggano l'integrità del sistema.

Anche i dispositivi mobili che abitano le nostre tasche e le nostre borse vanno tenuti costantemente aggiornati, e bisogna ricordarsi di farlo non solo per le app, ma anche per il sistema operativo (Android o iOS per citare i più famosi). È consigliato installare anche su di essi un sistema di antivirus: gli attacchi per ora non sono molti, paragonati a quelli sferrati contro i sistemi operativi, ma saranno sicuramente più frequenti nel prossimo futuro. Si può scegliere la versione gratu-

ita, facile da trovare online (attenzione però alla fonte da cui si scarica), ma se si usano questi device per uso professionale è opportuno acquistare la versione pro.

Capitolo 6 – Essere ricattati: i ransomware

Subire un ricatto (*ransom*, in inglese) nell'epoca digitale è più semplice di ciò che pensiamo, e gli ingredienti sono sempre gli stessi: fiducia mal riposta, disattenzione e l'inganno messo in atto da parte di terzi con tecniche spesso subdole. Ecco dunque che ci ritroviamo sotto scacco: gli hacker bloccano i nostri dispositivi e per riavere l'utilizzo degli stessi e i nostri dati dobbiamo pagare un riscatto. Casi eclatanti di ransomware andati a buon fine (per gli attaccanti, si intende) sono stati e sono all'ordine del giorno, aziende che pur avendo adottato tecniche di protezione, si sono trovate a pagare riscatti cospicui per riavere i propri dati.

Quello dei **ransomware**, ossia i software malevoli che criptano il contenuto di un hard disk o di un sistema e chiedono un riscatto per poterlo decifrare, è un fenomeno in continua crescita. Questo tipo di malware è sempre più aggressivo: spesso non si limita a cifrare i dati presenti sull'hard disk principale del computer colpito, ma va alla ricerca di eventuali hard disk esterni collegati, oppure di cartelle di Rete, al fine di cifrare anche i dati presenti in questi dispositivi per procurare il maggior danno possibile. Ci si aspetta che nel prossimo futuro prenderanno di mira anche i dati memorizzati nel cloud. Solitamente si hanno pochi giorni per provvedere al pagamento del riscatto, prima che la cifra aumenti o che i malviventi scompaiano lasciando i file illeggibili.

Seppur meno diffusi, i ransomware esistono **anche per i dispositivi mobili**. Grandi aziende che operano in settori diversi tra loro hanno subìto attacchi di questo tipo: il più noto è stato quello del malware "WannaCry", ma non è stato il solo. In alcuni casi le aziende hanno dovuto persino fermare l'attività per più giorni a causa dell'annientamento dei computer, anche se l'informazione del blocco della produzione non ha fatto notizia e non è arrivata sui media. La produzione e la diffusione dei ransomware sono un vero business: nel dark web esistono addirittura kit per creare direttamente online il proprio malware personalizzato senza bisogno di saper programmare. Alcuni di questi kit sono gratis per l'utente: lo sviluppatore terrà per sé una percentuale su ogni vittima che pagherà il riscatto e il resto verrà consegnato all'utente del kit che mette in atto la propagazione.

Per difendersi è necessario un buon **antivirus con protezione in tempo reale** e costantemente aggiornato.

Si consiglia di diffidare delle e-mail contenenti allegati di dubbia provenienza. Come ultima cosa, ma non per importanza, bisogna ricordare di effettuare backup periodici: in caso di infezione sarà possibile ripristinare i dati direttamente dal backup, senza essere costretti a pagare un riscatto. Il disco di backup non dovrà essere perennemente in linea con il computer, ma sarà collegato solamente quando necessario: in questo modo si evita che il virus intacchi anche i dati di backup.

Un altro tipo di minaccia che si diffonderà in futuro riguarda il controllo dei dispositivi informatici per

minare le criptovalute. Questo tipo di attacco avviene, banalmente, visitando pagine web infette, oppure appositamente create per sfruttare la CPU e/o GPU del dispositivo del visitatore. In questo modo non viene infettato il sistema ma se ne sfruttano le caratteristiche hardware. L'utilizzo elevatissimo della CPU o della GPU fa aumentare anche i consumi energetici e fa diminuire in modo molto rapido la batteria del dispositivo nel caso in cui non sia collegato a Rete elettrica. Essendo un attacco tramite browser web, sono colpiti indistintamente sia i computer sia i dispositivi mobili. Solitamente nei computer si nota un aumento della rumorosità della ventola, mentre nei cellulari e nei tablet si nota un surriscaldamento del dispositivo e un rapido scaricamento della batteria. Per proteggerci possiamo installare antivirus che implementino una protezione specifica oppure utilizzare estensioni del browser che siano in grado di bloccare gran parte del codice malevolo.

I sistemi industriali, già presi di mira svariate volte, continueranno a essere nel mirino degli hacker e ci si aspetta un'intensificazione degli attacchi agli strumenti OT (Operation Technology), che presiedono i sistemi di controllo delle reti, sistemi di monitoraggio e automazione dei trasporti. Oltre alle aziende attaccate per sottrarre dati, anche a fini di spionaggio industriale, verranno prese di mira quelle che si definiscono "infrastrutture critiche", come centrali elettriche ed atomiche. Attacchi a questi obiettivi sono già avvenuti in passato, fortunatamente senza arrecare gravi danni. Le strutture critiche, se non adeguatamente protette e

a maggior ragione se relativamente vecchie, sono un bersaglio interessante per i malintenzionati. E non finisce qui: si ipotizza che verranno scoperte nuove vulnerabilità anche su mezzi di trasporto obsoleti come ad esempio navi, treni o aerei che non implementano adeguati sistemi di protezione. È ad esempio accaduto che, in un test messo in atto su commissione dell'armatore, una società di sicurezza sia riuscita a violare una petroliera, inserendosi virtualmente nel sistema di controllo della nave, utilizzando come ingresso il protocollo di tracciamento in tempo reale: la banale password di default non era stata modificata dopo l'installazione del sistema!

Restando in ambito di trasporti, un tipo di attacco in costante crescita è quello ai danni delle autovetture più moderne, dotate di sistemi informatici di controllo. Non parliamo solo di attacchi informatici che permettono di controllare accelerazione, sterzo, freno, ecc.; ci sono attacchi messi in atto per rubare con facilità il veicolo. Ci riferiamo ai veicoli che usano la cosiddetta "smart key", ossia quella chiave che va avvicinata alla portiera per aprire il veicolo e avviarlo senza bisogno di inserirla nel quadro. I ladri, per poter aprire e mettere in moto il veicolo dotato di smart key, usano due ripetitori, uno che viene posto vicino alla portiera del veicolo, l'altro in prossimità della chiave originale del veicolo che vogliono rubare, solitamente nei pressi della porta d'ingresso. In questo modo il segnale della chiave viene replicato fino ad arrivare alla portiera dell'auto permettendone l'apertura: l'auto si apre perché "crede" di avere la smart key vicina

e tutto funziona come di consueto. Una volta messa in moto la macchina, la si può portare via a patto di non spegnerla. Le auto dotate di sistemi per le smart key sono infatti progettate per poter funzionare, una volta avviate, anche senza chiave, e questo per motivi di sicurezza: pensate a che cosa succederebbe se per un qualsiasi motivo la macchina si spegnesse durante il suo tragitto solo perché c'è stata una perdita di segnale tra l'autovettura e la chiave. Proteggersi in questo caso è semplice: è sufficiente acquistare appositi contenitori o piccole bust che hanno al loro interno una speciale schermatura per bloccare i segnali elettrici. Così custodiremo la chiave del nostro veicolo e saremo sicuri che non comunichi con niente.

Capitolo 7 – Furto con destrezza, e… senza contatto

Ormai diffusissime e usatissime, le carte di credito contactless, cioè quelle card che utilizzano la tecnologia NFC (Near Field Communication) per effettuare piccoli pagamenti senza dover inserire alcun PIN e senza dover firmare nulla, ma semplicemente avvicinando la carta a un POS, aprono scenari di attacco inquietanti. Appositi scanner permettono di leggere le carte senza nemmeno doversi avvicinare troppo e, tramite la scansione, consentono di leggere anche i dati. La tecnologia NFC è sfruttata non solo per le carte di credito: pensiamo alla chiave della camera di molti hotel, una tessera contactless che viene avvicinata alla maniglia della porta per aprire; ai tesserini universitari smart che permettono di accedere alle strutture dell'università come studenti o come docenti; persino i passaporti rilasciati negli ultimi anni hanno al loro interno questo tipo di tecnologia. Tutte queste tessere sono vulnerabili ai furti di dati, perpetrati usando apposite strumentazioni a una distanza sufficiente per non destare sospetto nella vittima. Per proteggersi, così come abbiamo visto per le smart key nel capitolo precedente, è sufficiente inserire le carte e il passaporto in custodie che schermano le tessere grazie a un rivestimento metallico interno.

Non dimentichiamo infine che, su dispositivi obsoleti e/o non aggiornati, anche la tecnologia Bluetooth potrebbe essere utilizzata da malintenzionati o cyber

criminali per eseguire codice malevolo e di conseguenza accedere e/o sottrarre dati dal dispositivo stesso. Pertanto, sia il Bluetooth sia l'NFC dovrebbero essere disabilitati in caso di non utilizzo.

Capitolo 8 – Abboccare nel (mare) digitale

I malware, di cui abbiamo trattato fino ad ora, sono il punto di arrivo della strategia dei malintenzionati digitali. Ma come arriva un malware fino ai nostri dispositivi connessi in Rete? Le modalità fraudolente oggi più diffuse attraverso le quali questo avviene ricadono sotto il nome di *phishing*.

Il termine è una variante dell'inglese *fishing*, che letteralmente significa "pescare". Dunque, i malintenzionati pescano nel mare digitale, nella speranza che qualcuno abbocchi.

Chi sono le vittime del phishing? Potenzialmente ogni utente della Rete. Alcune vittime, poi, vengono scelte per la particolare posizione che occupano all'interno di organizzazioni private o pubbliche, mentre altre sono scelte per la loro particolare debolezza.

Che cosa si "pesca" attraverso il phishing? Principalmente denaro, dati e persone. Delle prime due tipologie si parlerà più avanti. Qui si vuole brevemente accennare alla terza tipologia: le persone. La Rete è talvolta utilizzata per ingannare le persone più vulnerabili, ad esempio per adescare i più giovani. Anche questa attività, particolarmente odiosa, rientra nella definizione di phishing, ma gli scenari giuridici che apre sono molto diversi da quelli che riguardano la sicurezza informatica di cui questo lavoro si occupa e che dunque non approfondiremo, se non per esortare a prestare la massima attenzione.

Come si pesca? Si cerca di indurre la vittima a clic-

care su link o a connettersi a siti che nascondono strumenti per carpire i dati, oppure a siti che iniettano nei nostri dispositivi un qualche malware. Si può provare con una pesca a strascico, tirando su un po' tutto quello che capita, oppure si può preparare un'esca adeguata al tipo di pesce che si vuole pescare. Questi secondi attacchi sono i più pericolosi, perché può capitare che la vittima non si renda neppure conto di essere stata attaccata.

Quali sono gli strumenti con i quali si pesca? Le e-mail sono quelli prediletti, con cui spesso vengono compiuti attacchi complessi e persistenti (gli *Advanced Persistent Threat*, o APT). La vittima può anche essere indotta a lasciare i suoi dati per mezzo di siti costruiti *ad hoc*, oppure il suo device può essere infettato da malware che registrano tutta la sua attività.

La forma più popolare e datata di phishing è quella in cui il mittente ha bisogno dell'aiuto economico del destinatario per recuperare denaro, ottenuto più o meno lecitamente. Ovviamente, si promette una lauta ricompensa per l'aiuto una volta che il mittente avrà messo le mani sul malloppo. In questa categoria rientrano varie tipologie di mittenti e storie: il mittente si presenta come pubblico ufficiale di un qualche stato lontano che è stato in grado di stornare del denaro da fondi pubblici o privati. Oppure il mittente può essere un banchiere che sta cercando di chiudere il conto di un cliente morto di cui il destinatario è il parente più prossimo. Oppure il mittente è il parente di un militare o politico defunto che sta cercando di rivendicare un'eredità contro il governo che vorrebbe incamerare tutto.

Se rispondiamo ad uno di questi messaggi cadiamo nella trappola.

Il phishing via e-mail fa leva sul (falso) senso di fiducia che abbiamo nei confronti di un indirizzo e-mail che sembra attendibile e che dunque ci porta ad agire con leggerezza, di fatto ottenendo da noi comportamenti controproducenti, informazioni personali e dati riservati. Il phishing combina l'ingegneria sociale, ossia lo studio di come ci comportiamo per carpire informazioni da noi, a trucchi tecnici: un allegato nel messaggio di posta elettronica che carica un virus sul computer; un link a un sito che induce l'utente a scaricare malware o a consegnare spontaneamente le informazioni personali.

Quello che abbiamo appena illustrato è un invito a prestare maggiore attenzione a elementi che nella fretta quotidiana possono facilmente sfuggire quando usiamo l'email: non verifichiamo l'indirizzo del mittente e rispondiamo, magari dando dati sensibili come le credenziali di accesso alla banca online; scegliamo password troppo semplici (magari la stessa per più account o dispositivi, una pratica più diffusa di quanto si pensi, ma che è assolutamente da evitare) e questo facilita l'azione degli attaccanti. La comunicazione online, tanto comoda e veloce, ci impone di alzare la guardia, ma in un modo che non è poi così diverso da quanto già facciamo nella nostra vita "reale". Dunque, partiamo dai fatti: l'aumento continuo di dispositivi e persone connessi corrisponde ad un aumento dei raggiri digitali. E prendiamo le protezioni che servono.

Una topologia degli attacchi di phishing

Si possono individuare quattro dimensioni indipendenti con le quali è possibile descrivere gli attacchi di phishing sino ad ora noti.

La prima dimensione riguarda il supporto attraverso il quale l'attacco viene sferrato. L'attacco può essere portato attraverso un supporto fisico (ad esempio abbandonando delle pennette USB che contengono del malware) oppure attraverso la Rete (ad esempio attraverso una e-mail o compromettendo il server).

La seconda dimensione riguarda il mezzo attraverso il quale l'attacco viene sferrato; possono essere email oppure malware (ad esempio, un keylogger) le informazioni sulla macchina della vittima oppure, per finire, può essere stato compromesso un server o un servizio al quale la vittima si connette.

La terza dimensione riguarda coloro ai quali l'attacco è rivolto. L'attacco può essere indiscriminato e in questo caso il target sono potenzialmente tutti gli utenti in possesso di un indirizzo email e più in generale di una connessione alla Rete; oppure l'attacco può essere rivolto a coloro che appartengono a una specifica organizzazione anche se il target è l'organizzazione e non la persona specifica; per finire, l'attacco può essere rivolto a una persona specifica con l'intento di carpire i suoi dati.

La quarta dimensione riguarda il fine per cui l'attacco è stato sferrato. Gli attacchi, come si è già detto, vengono sferrati o per truffare la vittima oppure per estorcergli dei dati.

Tutti questi attacchi inducono con l'inganno l'utente a trasmettere i propri dati o le informazioni riservate in luoghi e a persone a cui non dovrebbero essere trasmessi. Alcuni di essi si possono prevenire tenendo sotto stretto controllo hardware e software. Per altri invece ciò non è sufficiente, perché l'hacking non è di tipo tecnico, ma cognitivo. Questo tipo di attacchi è quello che si sta diffondendo sempre di più e dà ottimi risultati perché le vittime sono, nella maggior parte dei casi, semplici utenti dei sistemi. È quindi necessario fare in modo che gli utenti siano in grado di difendersi da attacchi di tipo cognitivo prendendo coscienza dei pericoli impliciti nell'uso delle tecnologie dell'informazione.

Perché cadiamo vittime del phishing?

Nonostante quello che pensiamo di noi stessi e dei nostri simili, non sempre prendiamo decisioni razionali e logiche; ci sono fattori di carattere cognitivo, emotivo e contestuale che influenzano le nostre scelte. I phisher cercano di capire come prendiamo le decisioni e cercano di manipolare le condizioni per spingerci a compiere scelte sbagliate.

Per cercare di comprendere il problema bisogna tenere conto del fatto che l'uomo utilizza protesi che sono in grado di estendere non solo le sue capacità fisiche, ma anche le sue capacità cognitive. Il linguaggio, la scrittura, la lettura, l'aritmetica, la logica sono strumenti che ci permettono di estendere, ad esempio, la nostra capacità di ricordare, grazie alla possibilità di fissare all'esterno in maniera indelebile e oggettiva i

nostri ricordi, lasciando segni sulla carta per mezzo di matite o dentro gli hard disk dei computer. Secondo alcuni autori, qualunque entità tecnologica inventata dall'uomo al fine di potenziare il suo pensiero e ampliare il raggio delle sue azioni è un artefatto cognitivo e deve essere considerata parte di una cognizione estesa. In questo senso ogni tecnologia è un artefatto cognitivo progettato, realizzato, utilizzato dall'uomo e deve essere compresa in relazione alla sua interdipendenza dagli esseri umani; la tecnologia non è solo un potenziamento ma anche un completamento delle capacità umane. Di conseguenza, il limite tra le proprietà cognitive dell'individuo e le proprietà delle sue protesi tecnologiche non è un confine definito, ma varia a seconda dei contesti tecnologici e delle azioni che l'individuo pone in essere.

Quindi la tecnologia vive nel paradosso: essa da una parte rende la vita più semplice, offrendo numerosi vantaggi, dall'altra cresce in complessità, offrendo sempre più possibilità e diventando via via meno controllabile. È proprio il caso che si verifica con le email: il vergare una lettera su carta e il digitare una mail sono, al di là del nome, due attività che hanno in comune solo il nucleo centrale, lo scrivere e la volontà di inviare un messaggio a un'altra persona. Ma, ad esempio, inviare una lettera per sbaglio era, se non impossibile, molto raro, anche se la gestione quotidiana della corrispondenza poteva essere una cosa piuttosto complicata e non priva di problemi: dalle catene di sant'Antonio alle truffe.

Una delle più famose truffe diffusa oggi via mail, la truffa alla nigeriana, ebbe origine nel XIX secolo ed era nota come la truffa del prigioniero spagnolo: il truffatore diceva alla sua vittima di essere (o di essere in corrispondenza con) una persona ricca di alto lignaggio imprigionato in Spagna, sotto falsa identità; il prigioniero non poteva rivelare la sua identità senza subire gravi ripercussioni e si affidava a un amico (il truffatore) per raccogliere fondi per ottenere la sua liberazione; una volta libero coloro che avessero contribuito alla sua liberazione sarebbero stati generosamente ricompensati. Ovviamente, la diffusione era molto più lenta, i costi per metterla in atto più elevati, il numero di persone colpite molto più basso, ma evidentemente funzionava perché nel corso del XX secolo essa si ripresentò sotto varie forme, fino all'esplosione avvenuta negli anni 90 grazie alla diffusione della posta elettronica. Con il passare del tempo, grazie a una diffusa informazione, questa forma di truffa ha perso la sua efficacia, anche se ogni anno sono ancora migliaia le persone che, incredibilmente, ci cascano.

Che cosa caratterizza gli attacchi di phishing che utilizzano l'email? In primo luogo il testo della mail cerca di comunicare un grande senso di urgenza per indurre l'utente a compiere un errore; poi si chiedono spesso informazioni che il mittente dovrebbe già conoscere; vengono richieste credenziali d'accesso; si fa pressione affinché vengano aggirate le procedure standard che si seguono per eseguire un lavoro; il messaggio arriva apparentemente da una persona nota.

Capitolo 9 – Smart Working, alcuni spunti

La sicurezza delle informazioni e dei nostri dati è un argomento che ci riguarda sempre e dovunque, anche laddove la soglia di attenzione dovesse abbassarsi perché ci troviamo in luoghi che riteniamo sicuri come le nostre case, stanze e appartamenti.

Dal momento in cui si è connessi in Rete, qualunque sia il motivo (lavoro, studio, svago) l'attenzione ai rischi digitali va tenuta alta benché ci si senta sicuri e tranquilli nel salotto di casa.

A causa della situazione sanitaria del 2020 ci si è ritrovati improvvisamente a lavorare da casa, utilizzando a volte strumenti personali, in situazioni ove le norme di sicurezza stabilite dall'azienda erano difficilmente replicabili. Queste circostanze hanno però il merito di aver portato alla luce un aspetto positivo: si è avviato un processo di consapevolezza sui temi della sicurezza che ha aiutato le persone a comprendere quanto, anche al di là del lavoro, vada considerato il tema della cybersecurity.

Molte aziende si sono impegnate per mettere in sicurezza il lavoratore e gli strumenti da esso utilizzati in modalità (comunemente detta) di *smart working*.

Le restrizioni dovute all'emergenza sanitaria hanno accelerato l'adozione di una modalità di "lavoro a domicilio" che prima era quasi attività elitaria appannaggio di determinati ruoli aziendali, portandosi appresso una seppur sommaria, e poco strutturata, formazione alle persone nell'uso in sicurezza degli strumenti di lavoro.

L'accesso diretto a Internet con i device personali

Il fattore emergenziale ha fatto sì che in una prima fase si usassero dispositivi personali per attività di lavoro, aprendo però delle voragini di sicurezza risolte utilizzando connessioni VPN dove le comunicazioni sono criptate e gli utenti vengono autenticati prima di stabilire una connessione alla Rete aziendale. Tecnicalità e diffusione di politiche di sicurezza che hanno richiesto alle persone ulteriori addestramento sull'uso dei dispositivi connessi, con un vantaggio personale duraturo, una conoscenza e consapevolezza utilizzabile anche nella sfera privata delle persone.

Le raccomandazioni delle aziende hanno quindi aiutato le persone ad aumentare la propria consapevolezza d'uso anche nel privato. È bene sottolineare che queste modalità hanno riguardato solo una piccola parte delle aziende; molte attività sono e devono essere svolte in presenza e di conseguenza questo addestramento forzato, passato peraltro sottotraccia, è stato destinato ad una minoranza se si guarda alla totalità della forza lavoro dell'Italia o di qualsiasi altra economia sviluppata.

Capitolo 10 – Firma Elettronica e Posta Elettronica Certificata

Quando si parla di sicurezza dell'identità di chi abbiamo davanti nel mondo digitale, e di conseguenza di certezza che il documento che abbiamo ricevuto sia firmato da una persona con identità confermata, ci si trova ad affrontare il tema delle firme elettroniche e della posta elettronica certificata, due strumenti che irrobustiscono la sicurezza delle nostre comunicazioni digitali e che ci aiutano a comprendere la veridicità di quanto riceviamo.

Purtroppo, anche questi strumenti non sono esenti da abusi e usi malevoli: talvolta la causa è la stessa persona detentrice dell'indirizzo che incautamente lascia le credenziali a disposizione di terzi; altre volte le cause sono identificabili in attacchi mirati a cui non sono seguite contromisure atte a ristabilire la sicurezza violata.

Firme elettroniche e identità digitale

Con l'avvento dell'era digitale, molte esigenze tipiche del mondo analogico, gestite attraverso regole e abitudini consolidate in anni di onorato ed efficace servizio, hanno richiesto un ripensamento o un cambiamento importante. In questo contesto, un ruolo assolutamente centrale è stato svolto dagli strumenti digitali di "sottoscrizione" e "identificazione".

Sottoscrizione e Identificazione

Chiariamo meglio che cosa si intende quando si usano i termini "sottoscrizione" e "identificazione". Partiamo da quest'ultima.

L'identificazione è quel processo che, esaminando diversi elementi, consente di effettuare un chiaro riconoscimento ed attribuire con certezza un'identità. A volte è un processo esplicito, come quando ci viene richiesta la Carta di Identità in aeroporto e viene esaminata l'effettiva corrispondenza tra la foto e i dati riportati con la persona esaminata. Altre volte è un processo "implicito", in cui una persona, che già ci conosce, sa chi siamo e pertanto si comporta con noi in modo coerente: per esempio, quando in banca un addetto allo sportello ci riconosce e ci "identifica" come correntisti; oppure quando andiamo dal nostro medico, che ci visita.

Nel mondo analogico l'identificazione è una procedura consolidata e abbastanza semplice da effettuare: ci sono tutti gli strumenti necessari. Nel (nuovo) mondo digitale, invece, non è altrettanto scontata: da remoto, infatti, dobbiamo identificare qualcuno che richiede l'accesso a dati "sensibili", su cui è meglio, opportuno e a volte addirittura obbligatorio sincerarsi della corretta identità per non commettere errori.

La sottoscrizione è una modalità adottata per raccogliere esplicite "approvazioni". Il termine stesso ne identifica la natura (scritto-sotto) e lo strumento principe con cui viene praticata è l'apposizione di una firma. Nel mondo analogico, stiamo parlando della firma autografa, quella personalissima modalità con cui

ciascuno di noi scrive il proprio nome e cognome. Un documento o una richiesta in carta, "firmati" raccontano immediatamente e a chiunque che la persona che ha messo lì la sua firma "crede" nei contenuti che vi sono riportati sopra, li fa propri e li autorizza.

Sempre nel mondo analogico, la firma è una scritta, a volte avvalorata ulteriormente da altri strumenti di garanzia che favoriscono l'effettiva identificazione dell'autore della firma stessa. Per esempio, un sigillo (apposto con la ceralacca), oppure un timbro che marca il documento e attesta ulteriormente la paternità di quella firma. Nel (nuovo) mondo digitale, la sottoscrizione non può essere apposta "a mano" ma solo digitalmente. Così, però, perde le sue caratteristiche "personalissime" di riconoscibilità, riconducibili all'autore. Quindi questo strumento deve essere ripensato per adeguarsi alle dinamiche del digitale, anche profondamente. Così è stato, e da questo processo sono derivate diverse tipologie di firme elettroniche.

Per gestire sottoscrizione e identificazione in modo chiaro e univoco, riconosciuto non solo in una regione o in un paese ma (almeno) in tutta Europa, è stato addirittura emanato un "regolamento" (a dispetto del nome abbastanza banale, si tratta di uno strumento legislativo estremamente potente a disposizione dell'Europa, capace di sovrascrivere, in caso di incongruenze col quadro legislativo di un qualsiasi singolo paese aderente, la legislazione locale a favore di quando previsto nel regolamento stesso). Si tratta del regolamento UE n° 910/2014, chiamato anche eIDAS (electronic IDentification Authentication and Signature), che

definisce una base di regole per abilitare interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni, puntando sulla sicurezza e sull'efficacia dei servizi elettronici e delle transazioni online (di commercio elettronico tra imprese e verso i consumatori) in tutta l'Unione Europea.

L'identificazione digitale

Identificare qualcuno nel mondo digitale significa accertarsi "prima" che la persona con cui si interagisce sia effettivamente autorizzata ad "accedere a" e "compiere azioni su" determinate informazioni "a sua esclusiva disposizione" oppure "di sua proprietà" (dati personali, pagamenti, diagnosi mediche, ecc.).

Nel mondo bancario, queste procedure di identificazione sono state alla base dello sviluppo dei sistemi di remote banking per consentire il log-in in ambienti dai quali è possibile manovrare conti e pagamenti. Sulla base di regole definite dal sistema bancario per garantire la sicurezza degli utenti, sono stati sviluppati sistemi di identificazione basati su più strumenti (un computer, un cellulare, un token, ecc.), su più password (predefinite, modificabili, temporanee, a volte "one-time" ovvero usabili una sola volta) che sono onerosi e complessi da gestire ma che effettivamente salvaguardano concretamente la nostra sicurezza (o almeno ci provano seriamente!). Ogni banca ha sviluppato un proprio modello di riconoscimento e fa da garante che le informazioni in grado di attivarlo siano "al sicuro". Questa specificità dei meccanismi di identificazione, tuttavia, non poteva rimanere appannaggio

di ogni singola istituzione o ente capace di erogare servizi ai cittadini: questo, infatti, comporterebbe un incontrollato proliferare di password (già oggi spesso se ne gestiscono fin troppe…) e un pesante costo di gestione per chiunque eroghi servizi "personali" online.

Da queste riflessioni, quindi, si è pensato di "tirare fuori" i sistemi di identificazione e renderli un "servizio digitale" a parte, regolato e garantito da alcuni operatori e adottabile da più interlocutori diversi sulla base di specifiche regole. Molti paesi europei hanno scelto le loro modalità per garantire sicurezza ed efficacia di identificazione. L'Italia ha scelto di introdurre il sistema "SPID" (Sistema Pubblico per l'Identità Digitale) che consente l'accesso a una gran quantità di servizi pubblici ed è a disposizione anche di operatori privati che intendano usarlo come strumento di accesso per i loro servizi online.

In estrema sintesi, SPID prevede: (i) un'identificazione forte in fase di registrazione iniziale, che può avvenire anche da remoto ma richiede di mostrare la carta di identità e la propria faccia in un'intervista via web/videocall con un operatore che ha la responsabilità di identificarci; (ii) il conferimento di un identificativo personale e di una password temporanea che, una volta associata all'identificativo, consente ai sistemi di autorizzare l'accesso ad ambienti e informazioni riservate solo al proprietario di quell'identità. I certificati SPID vanno, nel tempo, rinnovati: a garanzia che l'identità sia sempre nelle mani di chi effettivamente rappresenta.

La sottoscrizione elettronica (e le varie firme elettroniche)

Nel passaggio da analogico a digitale, anche lo strumento della firma ha dovuto subire importanti trasformazioni. Una firma autografa si porta dietro due forti "informazioni": identifica puntualmente chi l'ha scritta e avalla la piena condivisione o autorizzazione, da parte dell'autore, dei contenuti nel documento sotto al quale viene "vergata". Come trasferire queste due fondamentali informazioni in un mondo digitale, che per natura perde alcune caratteristiche fondamentali (come la "personalità del tratto") di riconoscibilità? Lavorando normativamente e, in primo luogo, invertendo l'ordine della "prova". Vuol dire che nel mondo analogico una firma può sempre essere disconosciuta: se viene disconosciuta, giuridicamente spetta poi a un giudice stabilire se quella firma è o non è della persona che rappresenta. Il giudice riesce in questo complicato sforzo affidandosi a periti che analizzano la calligrafia e sulla base di molti parametri (lo stile, il tratto dell'autore, l'indice di pressione, la presenza di vezzi o greche…) possono stabilire se la firma è di chi l'ha disconosciuta o meno. Se lo è, lo è e basta: non può più essere disconosciuta. Se non lo è, non lo è. Nel mondo digitale, la gran parte di questi parametri viene completamente persa. E allora, per dare valore a una firma elettronica (in particolare nelle sue forme più forti come quella "qualificata" o "digitale"), si "inverte" l'onere della prova, cioè una firma elettronica non può essere disconosciuta dall'autore (la firma digitale che riporta quel nome e che è stata affidata a quella

persona da una Certification Authority – i provider che vendono le firme digitali – è senza alcun dubbio di quella persona). All'autore, e non al giudice, spetta l'onere di provare di non essere stato lui ad apporre quella firma su quel documento informatico.

Una volta sganciati dalle "zavorre normative" che non consentirebbero di passare dall'analogico al digitale, la firma elettronica diventa "attuabile" ed estremamente "potente".

Esistono tre tipologie principali di firme elettroniche, che si differenziano in base alla loro "valenza giuridica" per l'opponibilità a terzi. La forma più blanda viene chiamata firma elettronica semplice. Si tratta di una forma di sottoscrizione in qualsiasi modo riconducibile a qualcuno. L'esempio più facile è l'immagine di una firma autografa, copiata in calce a un documento (in fondo, chiunque potrebbe scansionarla e apporla in quella posizione, non necessariamente solo il suo autore; ed essendo priva delle caratteristiche di una firma autografa – pressione sulla carta, caratteristiche dell'inchiostro, ecc. – non può avere né le sue proprietà né la sua valenza). Questo è l'esempio facile ma nel mondo digitale ce ne sono anche molti altri: per esempio una mail, inviata da un indirizzo riconoscibile, è assimilabile per valenza a una firma elettronica semplice. Persino un flag su una cella, all'interno di una sessione di lavoro in cui ci si è resi più o meno riconoscibili, può rappresentare una firma elettronica semplice. Ovviamente la sua valenza giuridica è molto bassa, fortemente interpretabile e da approfondire nelle sedi opportune, se necessario.

La firma più forte è invece la firma elettronica qualificata o firma digitale. È la firma che ci viene rilasciata da una Certification Authority, può essere su una chiavetta oppure in cloud e accessibile da remoto e viene attivata con un articolato percorso di password e strumenti di riconoscimento. Questa è la firma giuridicamente più forte: si raccomanda sempre di tenerla sotto controllo, quindi, e di trattarla con riservatezza. Se qualche malintenzionato ne venisse in possesso, potrebbe crearci molti problemi (spetterebbe a noi dimostrare – come? – che non l'abbiamo usata per quella circostanza…). Nonostante sia fortemente consigliato presidiarla direttamente, l'idea ingenua che una firma digitale appartenga al mondo degli strumenti informatici e non strettamente e in modo univoco alla persona a cui è stata rilasciata, ha introdotto la deprecabile e azzardata abitudine di affidarne l'uso a persone supposte "di fiducia", nella speranza che se ne prendano cura come e quanto dovrebbe il legittimo proprietario: molti commercialisti o avvocati o segretarie di piano hanno infatti spesso cassetti pieni di credenziali, chiavette e password…

Sempre il regolamento eIDAS ha introdotto anche la firma elettronica avanzata (o FEA). Questa firma ha la stessa forza giuridica della firma digitale ma, contrariamente a questa, non è uno strumento: è un processo! In estrema sintesi, una firma elettronica avanzata può essere una qualsiasi tipologia di firma (anche quella semplice!) apposta all'interno di un processo che prevede, nella sua fase iniziale, una procedura forte di identificazione digitale. Per esempio, l'accesso a un

sito con SPID identifica in modo forte l'identità di chi sta entrando. Una volta entrati, una procedura guidata che porta l'utente ad apporre un flag può far considerare questa azione come un'approvazione firmata (digitalmente) da parte dell'utente stesso. La firma elettronica avanzata, se ben progettata, è probabilmente la forma più efficace e "naturale" per la raccolta di firme in formato elettronico.

Va infine accennato che, accanto alle firme elettroniche qualificate, sono stati recentemente introdotti da eIDAS anche i sigilli elettronici qualificati. Sono tecnologicamente analoghi alle firme digitali ma servono per la sottoscrizione delle persone giuridiche (le aziende, di cui riportano denominazione, partita IVA, codice fiscale).

L'insieme degli strumenti di sottoscrizione si completa con le "marche temporali": tecnologicamente sono paragonabili alle firme digitali ma in più riportano l'orario preciso in cui vengono apposte. Per questo motivo, un documento informatico non può essere marcato direttamente da chi lo produce, ma è necessario richiedere a terzi (come servizio), di praticarne l'apposizione. A fornire le marche temporali sono le Certification Authority, che con questo strumento "cristallizzano" il contenuto di un documento digitale nel momento stesso in cui questo viene marcato. L'adozione della marca temporale non solo fotografa il contenuto di un documento (che può essere firmato) in un preciso istante, ma ne consente anche la conservazione nel lungo periodo, all'interno del processo di conservazione digitale a norma.

Posta Elettronica Certificata

La PEC (posta elettronica certificata) è un'altra delle applicazioni giuridiche della crittografia asimmetrica. Dal punto di vista giuridico la PEC ha esattamente lo stesso valore di una raccomandata: così come non si può ignorare di aver ricevuto una raccomandata cartacea, se si possiede un indirizzo di posta elettronica certificata, non si può ignorare di aver ricevuto una mail certificata.

Il funzionamento della PEC è modellato esattamente su quello di un tradizionale lettera raccomandata: quando si va in posta per spedirla, l'ufficio rilascia al mittente una ricevuta che ha valore di data certa per la spedizione; posso cioè dimostrare giuridicamente che la lettera è stata spedita in quella data. Il postino prima di consegnare la lettera fa firmare colui al quale consegna la missiva. In questo modo il mittente di una raccomandata può dimostrare di aver spedito la lettera e può dimostrare che qualcuno al domicilio del destinatario l'ha ricevuta.

Allo stesso modo, quando si invia una PEC, per prima cosa si riceve una mail firmata dal sistema di spedizione che attesta l'effettivo invio, e poi si riceve un'altra mail, anch'essa firmata dal sistema di spedizione, che attesta che la mail inviata è stata effettivamente consegnata nella casella di posta del destinatario. A differenza della raccomandata non sia ha la certezza che il destinatario abbia contezza della presenza della mail nella sua mailbox; nonostante ciò, eventuali scadenze giuridiche decorrono dal momento in cui la mail è recapitata nella casella di posta.

Capitolo 11 – Cyberbullismo

Con Internet il bullismo, come molti altri comportamenti, si è trasferito nella dimensione virtuale dando origine al fenomeno del cyberbullismo, una nuova forma di persecuzione che viene messa in atto utilizzando i social network, le e-mail, le app di messaggistica, le chat e qualsiasi altro strumento o servizio digitale.

Come i bulli nella vita reale hanno a seguito qualche tirapiedi, il pubblico per i cyberbulli è il web: l'obiettivo del loro operato è quello di isolare una vittima e metterla in ridicolo, cercando il consenso di amici e follower sui social.

Mentre nei luoghi abitualmente frequentati dai più giovani il controllo e la supervisione degli adulti svolge un ruolo di garanzia e prevenzione verso atti di bullismo, sul web, data la sua natura intrinseca, è molto più complicato controllare che non si verifichino queste situazioni, e lo strumento più efficace per contrastarle è la prevenzione.

Qualora si dovesse arrivare a veri e propri atti di cyberbullismo, è molto importante parlarne con persone di fiducia, come genitori o insegnanti. Se non fosse possibile cercare l'aiuto di queste persone, anche solo per paura di essere giudicati, il telefono azzurro garantisce un canale sempre operativo per situazioni di questo genere.

Il cyberbullo, solitamente, sentendosi al riparo da conseguenze e ripercussioni grazie alla presenza di uno schermo tra sé e la vittima non si pone freni.

La legge definisce il cyberbullismo come qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via digitale, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo è quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso. In buona sostanza, il cyberbullismo consiste in una vessazione perpetrata ai danni di un minore attraverso il mezzo telematico.

Un attacco di cyberbullismo si può esprimere in varie forme ma il mezzo attraverso cui è commesso è sempre lo stesso: Internet.

Per tale ragione, la prima forma di tutela prevista dalla legge consiste nella possibilità di inoltrare al gestore del sito Internet o del social network una richiesta di immediato oscuramento, rimozione o blocco dei contenuti lesivi.

L'istanza di oscuramento del sito web può essere avanzata direttamente dalla vittima che abbia compiuto i quattordici anni oppure dai genitori. Il materiale non viene cancellato ma ne viene reso impossibile l'accesso agli utenti: in questo modo i contenuti potranno sempre essere utilizzati come prova sia dalla persona offesa che dalle autorità.

La nuova legge 71/2017 per la prevenzione e il contrasto del cyberbullismo prevede che le richieste di cancellazione dei contenuti vengano inviate al titolare del trattamento o al gestore del sito Internet o del

social media dove sono pubblicate le informazioni, le foto, i video, ecc. ritenuti atti di cyberbullismo.

Se il titolare del trattamento o il gestore del sito Internet o del social media che ospita i contenuti ritenuti offensivi non risponde entro 24 ore e non provvede alla richiesta di eliminazione entro 48 ore, ci si può rivolgere al Garante per la protezione dei dati personali, che entro 48 ore provvede in merito alla segnalazione. L'intervento del Garante contro atti di cyberbullismo può essere richiesto compilando ed inoltrando il modulo presente sul sito istituzionale dell'autorità.

Poiché il cyberbullismo, per precisa disposizione normativa, riguarda i minori, molto spesso i primi ad accorgersi delle condotte vessatorie o delle loro conseguenze sulle vittime sono gli insegnanti. Secondo il nostro ordinamento giuridico, il dirigente scolastico che viene a conoscenza di un episodio di cyberbullismo commesso da uno o più studenti del proprio istituto è obbligato ad informare immediatamente i genitori dei responsabili e a prendere adeguati provvedimenti disciplinari di carattere educativo.

La legge prevede che, al fine di prevenire e contrastare il fenomeno nelle scuole, operatori scolastici e forze dell'ordine debbano seguire un preciso corso di preparazione. Nello specifico, è prevista: la formazione del personale scolastico, con la partecipazione di un proprio referente per ogni autonomia scolastica; la promozione di un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'istituto scolastico in attività di prevenzione e contrasto del cyberbullismo nelle scuole; misure di soste-

gno e rieducazione dei minori coinvolti. Ogni istituto scolastico, poi, è tenuto ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.

Capitolo 12 – Come sopravvivere nell'era digitale

Abbiamo iniziato questa nostra breve trattazione usando le metafore della porta di casa lasciata aperta e dei mazzi di chiavi affidati a terzi, concetti che mirano a portare all'attenzione il tema della sicurezza nel nostro vivere e agire quotidiano onde evitare incidenti, pericoli, furti o altri atti criminali.

La diffusione degli oggetti digitali, della loro interconnessione continua, da anni ormai ha spalancato le porte a nuovi scenari del crimine.

Nei capitoli precedenti abbiamo passato in rassegna tecniche e minacce che rendono possibile ai malintenzionati penetrare nelle nostre sfere personali digitali, dal conto bancario ai fascicoli sanitari online, solo per citare alcuni esempi.

Nell'anno della pandemia si è registrato il record, negativo, di attacchi informatici. Siamo giunti a una condizione di quotidiano allarme rosso, condizione corroborata da accadimenti internazionali come gli attacchi informatici usati per aggredire nazioni e istituzioni: dal cybercrime alla cyberwar il passo è stato brevissimo, superando un confine che è sempre stato labile.

È altamente probabile che la situazione sia destinata ad aggravarsi poiché il cybercrime, a fronte di elevatissime opportunità di profitto, presenta un rischio di gran lunga più basso rispetto ad altre attività illecite, soprattutto perché, come abbiamo visto, è possibile

attaccare e recare danno ad una persona distante migliaia di chilometri.

Non c'è bisogno che si sfondi la porta blindata di un appartamento, o che il malintenzionato approfitti di una finestra lasciata aperta per entrare e fare razzia, perché può benissimo essere seduto ad una scrivania aspettando "che il pesce abbocchi", che apra una e-mail di phishing e inserisca, ad esempio, le sue credenziali per verificare l'account dell'home banking.

Quanto visto sino ad ora ha l'ambizione di farci riflettere sull'importanza della consapevolezza grazie alla quale è possibile ridurre drasticamente l'impatto del phishing, adottando un comportamento responsabile, ponendosi delle domande, prestando attenzione a ciò che ci capita di inusuale nelle interazioni con attori e oggetti digitali.

Chiudiamo con alcune indicazioni a cui prestare attenzione, già descritte in precedenza, ma che è bene riprendere in maniera sintetica.

Per approfondimenti segnaliamo al termine una serie di luoghi istituzionali dove è possibile trovare guide e precisazioni sui temi trattati.

- Leggere l'informativa privacy per verificare chi e come e perché gestirà i nostri dati personali.
- Fare attenzione ai consensi che diamo quando navighiamo o usiamo un'applicazione.

Questi due passi ci rendono consapevoli delle informazioni che abbiamo concesso a terzi,persone o aziende, e della finalità per cui saranno usate.

Quando riceviamo un e-mail che ha carattere d'urgenza o ci chiede di compiere azioni, poniamoci alcu-

ne domande:

- Il mittente dell'email è qualcuno che si conosce?
- L'e-mail per qualche motivo era attesa?
- L'indirizzo del mittente è corretto o è modificato per ingannare? (es: 0 al posto della "o" e "n" al posto di "m", ecc.)
- Le richieste che sono fatte nella mail sono ragionevoli e coerenti con le mie abitudini?
- Paura, avidità, curiosità sono stati che l'e-mail mi suscita per indurmi a compiere una particolare azione che altrimenti non farei?
- Se mi si chiede di fare una determinata azione, ho prima verificato contattando direttamente il destinatario o l'ente che rappresenta?
- Ho mai chiesto il contatto a chi mi scrive, e sono certo della sua identità?

I tentativi di phishing possono verificarsi anche via sms o via telefono. Apparentemente riceviamo un messaggio da un contatto istituzionale o da un numero registrato nella rubrica del telefono, mentre in realtà si tratta di malintenzionati che, per esempio, sono riusciti ad entrare nella Rete telefonica della banca e simulano chiamate da numeri affidabili. Nel dubbio è meglio contattare una persona di fiducia o la filiale e fare una verifica.

In alcuni casi è sufficiente inserire una parte del corpo della email sui motori di ricerca per trovare risultanze in merito alla truffa, oppure verificare che i link presenti nella email non siano fraudolenti e puntino ad altri siti non istituzionali.

Sicuramente le tecniche di cybercrime continuano

ad affinarsi, però più si affina la consapevolezza delle persone e la loro attenzione, più si mitigano i rischi.

Banche e altre istituzioni stanno promuovendo campagne di sensibilizzazione sul tema e introducendo ulteriori livelli di sicurezza, come, ad esempio, l'utilizzo di sistemi di doppia autenticazione.

La sicurezza informatica parte però dalla persona: siamo noi, adulti e minori, a trovarci per le mani oggetti nuovi e potenzialmente pericolosi.

Consapevolezza e responsabilità sono doti da esercitare e da tenere allenate.

L'arte dell'inganno e del raggiro a spese delle debolezze altrui esiste da sempre; quello che adesso sta cambiando è il contesto, anzi, i contesti, invisibili, immateriali, digitali appunto. Teniamo a mente, però, che i danni provocati, sia dal punto di vista economico sia da quello emotivo, sono tangibili e spesso molto rilevanti.

I temi del mondo digitale non si limitano a quelli toccati fin qui, tutti i giorni sentiamo parlare di Intelligenza Artificiale, Realtà Virtuale, Criptovalute e blockchain, e forse ci chiediamo come essere pronti per vivere in sicurezza in questo Nuovo Mondo in continua trasformazione. Questo quaderno è il punto di partenza per affrontare il viaggio.

Per approfondire le tematiche affrontate

I seguenti link rimandano a contenuti utili per approfondire le tematiche affrontate, enti istituzionali nazionali ed europei in cui sono raccolti i più recenti aggiornamenti sulle normative in materia di protezione dati, sul cyberbullismo, sul phishing e sugli altri temi trattati in questo quaderno.

Qui un QR code per visualizzarli in maniera rapida:

Link	Sito
https://www.garanteprivacy.it/	Autorità Italiana – Garante Privacy
https://www.garanteprivacy.it/temi/cyberbullismo	Garante Privacy – Cyberbullismo
https://www.garanteprivacy.it/temi/cybersecurity/phishing	Garante Privacy – Phishing
https://www.enisa.europa.eu/	ENSA – Agenzia UE cybersecurity

https://edpb.europa.eu/edpb_it	Autorità UE – Data Protection Board
https://edps.europa.eu/_en	Autorità UE – Data Protection Supervisor
https://temi.camera.it/leg18/temi/sicurezza_cybernetica.html	Stratificazione normativa Perimetro cibernetico
https://www.sicurezzanazionale.gov.it/sisr.nsf/index.html	Sistema di informazione per la sicurezza della Repubblica – Agenzia Cybersecurity
https://www.miur.gov.it/bullismo-e-cyberbullismo	Fonti normative per iniziative contro cyberbullismo
https://www.garanteprivacy.it/temi/cybersecurity/phishing	Phishing – Vademecum Garante ITA
https://curia.europa.eu/jcms/jcms/j_6/it/	Corte di Giustizia dell'Unione Europea
https://ec.europa.eu/info/index_it	Commissione europea

CASSA RURALE
DI LEDRO
CREDITO COOPERATIVO ITALIANO

I valori delle nostre genti

I valori della mentalità e della solidarietà costituiscono le solide basi su cui poggia la Cassa Rurale di Ledro.

www.**cr-ledro**.net

CASSA RURALE
DI LEDRO
CREDITO COOPERATIVO ITALIANO

Le radici della nostra storia

Dal 1984 le nostre porte sono aperte al territorio e allo sviluppo economico, sociale e culturale della comunità.

www.**cr-ledro**.net

CASSA RURALE
DI LEDRO
CREDITO COOPERATIVO ITALIANO

La banca della comunità.

Ogni anno dedichiamo una quota dell'utile al sostegno di iniziative culturali, sportive e sociali. Lo facciamo perché siamo convinti che il nostro compito sia contribuire alla crescita e al benessere della società, supportando gli stimoli positivi che nascono dal territorio.

www.**cr-ledro**.net

CASSA RURALE
DI LEDRO
CREDITO COOPERATIVO ITALIANO

La forza di un grande gruppo

La Cassa Rurale di Ledro aderisce al Gruppo Bancario Cooperativo Cassa Centrale Banca. L'idea partita oltre 130 anni fa cresce forte come questo albero.

www.**cr-ledro**.net

ReD OPEN FACTORY - Center for Responsible Innovation è il Centro per l'innovazione responsabile creato da ReD OPEN.

Alimentiamo la diffusione, co-creazione e co-progettazione di **regole, modelli e metodologie operative** per un **utilizzo consapevole dei dati nei processi aziendali**.

Il Center for Responsible Innovation:

- **diffonde nelle imprese la ricerca** non ancora applicata e incentiva un modello di business orientato al trasferimento tecnologico permanente tra impresa, università e ricerca;
- Organizza tavoli di lavoro per **approfondire e indagare tematiche emergenti** nell'ambito della ricerca e trasferirne possibili applicazioni alle aziende;
- Abilita **logiche partecipative e condivise** per l'adozione di linguaggi e processi che sono potenzialmente innovativi ma non ancora applicati in modo diffuso.

ReD OPEN è uno spin-off partecipato dell'**Università di Milano-Bicocca**, nato con l'intento di accompagnare e aiutare le imprese per affrontare percorsi di innovazione, transizione digitale e ricorso all'Intelligenza Artificiale in modo «responsible by design». Con competenze ed esperienze multidisciplinari, ReD OPEN propone percorsi di accompagnamento e di riconfigurazione dei modelli organizzativi e di business, in chiave responsabile.

Per approfondimenti:
www.redopenletter.it
www.redopenfactory.com
www.redopen.it

Gli strumenti tecnologici sono parte integrante della vita quotidiana e proprio per tale ragione è bene che vengano utilizzati in modo sicuro e consapevole.
Lo scopo di questa introduzione all'educazione civica digitale è rendere consapevoli gli utenti dell'importanza della sicurezza informatica. È fondamentale conoscere i pericoli che si possono nascondere dietro il progresso tecnologico, "e liberarci dal malware".

Questo quaderno, co-finanziato da Cassa Rurale di Ledro – Banca di Credito Cooperativo –, è utile per capire meglio temi come ad esempio cybersecurity e privacy, divenuti ormai indispensabili nel mondo digitale.

Iniziativa del Centro Studi della ReD OPEN FACTORY in collaborazione con la Cassa Rurale di Ledro.

www.ledizioni.it

9 788855 266635

€ 9,90