Di chi sono i dati di una persona che non c'è più?

Paolo Attivissimo

È uno scenario che molti sono riluttanti ad affrontare ma che prima o poi capita praticamente a tutti: un familiare ci lascia per sempre. Chi gli sopravvive deve mettere ordine nelle cose e nelle attività del defunto. Burocrazia e formalità sofferte, alle quali oggi si aggiunge il problema dell'eredità digitale. Le regole di questa eredità sono diverse da quelle che molti si aspettano, ed è meglio conoscerle.

Corrispondenza, bollette, abbonamenti, contratti e iscrizioni a servizi sono sempre più in forma elettronica, e quindi chiudere un conto telefonico, un leasing o un contratto di fornitura di energia, o anche soltanto scoprirne l'esistenza, spesso richiede che gli eredi possano accedere alla mail, alla rubrica e ai vari account (per esempio WhatsApp) della persona deceduta.

Ma se gli eredi non conoscono le password di accesso a questi servizi e i codici di sblocco dei computer, tablet o telefonini della persona venuta a mancare, nei quali sono racchiusi tutti questi dati, tutto si complica enormemente. Il tradizionale raccoglitore di contratti e fatture, magari caotico ma certamente apribile da chiunque, viene sostituito da una cassaforte digitale sigillata e quasi inespugnabile.

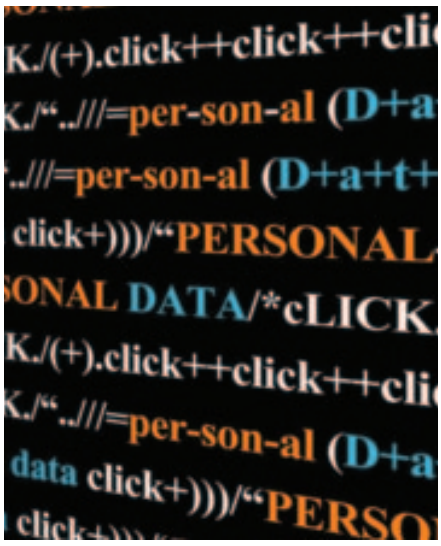
Dal punto di vista tecnico, ci sono vari modi per scavalcare quasi tutte queste protezioni. Alcuni sono semplici; altri sono molto più complicati e costosi, specialmente nel caso dei telefonini più moderni, le cui sofisticate difese, pensate per proteggersi dai ladri, rischiano di diventare una barriera inaspettata per i legittimi eredi che vorrebbero semplicemente mettere in ordine gli affari della persona scomparsa.

Rivolgendosi a esperti qualificati è quasi sempre tecnicamente possibile recuperare almeno in parte questi accessi, sia pure a costi spesso elevati e con il rischio che un errore di procedura cancelli tutti i dati. Questo è possibile anche nel caso di dispositivi protetti tramite impronta digitale o riconoscimento facciale.

Ma ci sono degli ostacoli importanti anche dal punto di vista legale che è opportuno conoscere e valutare per tempo. L'avvocata Katya Schober-Foletti, giurista dell'ACSI, che i lettori de La Borsa della Spesa conoscono bene, mi ha spiegato alcuni princìpi fondamentali.

Prima di tutto, mi ha chiarito, "una volta decedute, le persone, che non sono più persone, non hanno più, salvo rare eccezioni, diritti personali." È un fatto poco conosciuto e probabilmente sorprendente per molti, ma non legittima i familiari ad accedere a tutti i dati presenti per esempio sul telefonino del defunto. Infatti fra quei dati ci sono anche quelli delle persone viventi con le quali il deceduto ha avuto comunicazioni: indirizzi, numeri di telefono, fotografie e video, messaggi confidenziali, segreti professionali, eccetera. E quei segreti, essendo corrispondenza, sono tutelati dall'articolo 13 della Costituzione federale e dalla Legge Federale sulla Protezione dei Dati (LPD).

In secondo luogo, il PIN sul telefonino o la password sull'account sono considerati dalla legge dei "provvedimenti tecnici" atti a proteggere i dati personali contro un trattamento non autorizzato. La loro presenza indica l'intenzione della persona deceduta di proteggere quei dati. Ma è anche vero che molti telefonini e computer si bloccano automaticamente se non vengono usati e questo blocco è indiscriminato (si applica a tutti), e quindi è difficile capire se i familiari siano stati esclusi dall'accesso intenzionalmente o se il defunto semplicemente non ci abbia pensato e siano scattati gli automatismi del dispositivo.



In un caso del genere e in mancanza di disposizioni specifiche della persona deceduta, spiega l'avvocata Schober-Foletti, un familiare "potrebbe adire la pretura e presentare una domanda di accesso adducendo al Giudice il suo interesse". Il Giudice dovrebbe poi soppesare questo interesse e valutare se sia preponderante rispetto a quello delle persone i cui dati sono racchiusi nel dispositivo. Insomma, non è una questione facile, e oltretutto la si deve affrontare in un momento delicato come quello del lutto.

Tutto questo si può evitare con piccoli gesti di previdenza, per esempio affidando PIN e password a una o più persone di fiducia e lasciando istruzioni precise. Ma mi raccomando: non memorizzatele dentro il telefonino.

Consigli ACSI

- Se volete che i vostri eredi o familiari abbiano accesso alla vostra mail e ai vostri profili sui social network, preparate una lista delle password, stampatela e mettetela in una busta sigillata da aprire solo in caso di emergenza. Non includete le password dei servizi che volete far dimenticare per sempre.
- Se usate Facebook, nominate un cosiddetto "contatto erede", come spiegato nel Centro assistenza online di Facebook. Si può fare lo stesso con Gmail, cercando "eredità digitale" nel proprio account, e con molti altri servizi.
- Non correte a chiudere il contratto cellulare della persona deceduta: potrebbe servirvi per ricevere gli SMS contenenti i codici di verifica o recupero dei vari servizi e abbonamenti.

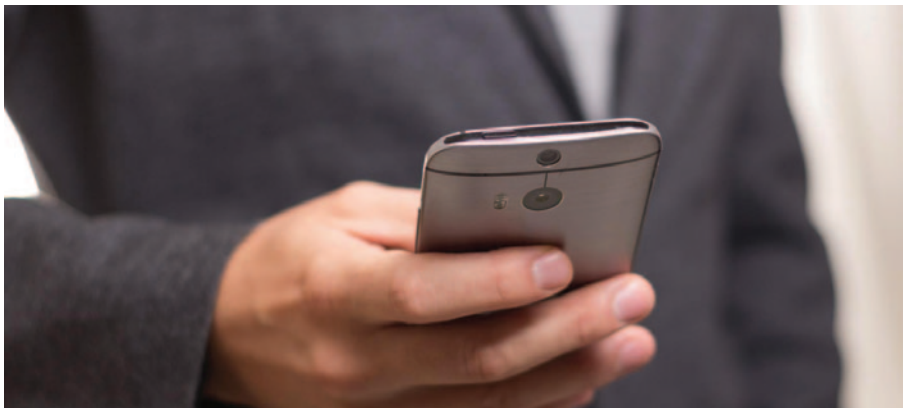
Perché le banche vogliono **farci usare le app?**

Paolo Attivissimo

Ci siamo da poco abituati, magari a malincuore e a fatica, a usare il computer per gestire i conti bancari, e adesso ci viene chiesto di cambiare di nuovo tutto. Al posto del sito della banca sul computer, arriva l'app sul telefonino. Sempre più spesso le banche propongono ai propri clienti di scaricare un'app appositamente realizzata e usarla per tutte le transazioni.

Ma gli utenti sono spesso riluttanti ad accettare questa proposta, non solo perché devono imparare un nuovo modo di fare le cose ma anche perché lo schermo del telefonino è piccolo e poco leggibile e la tastiera è minuscola, per cui è facile sbagliare. In più il telefonino viene percepito come meno sicuro rispetto al computer, perché lo si porta in giro ed è quindi più facile danneggiarlo, smarrirlo o vederselo rubare insieme all'accesso al conto bancario. Ci sono anche correntisti che non hanno lo smartphone e non vogliono averlo perché il telefonino normale è sufficiente per le loro esigenze. Allora perché le banche ci tengono così tanto a spingerci verso le app?

La ragione fondamentale è la sicurezza dei nostri soldi. Può sembrare paradossale, ma usare sul telefonino l'app fornita dalla propria banca è molto più sicuro che usare un programma di navigazione (come Safari, Microsoft Edge, Google Chrome o Firefox). I criminali informatici hanno infatti creato molti modi per ingannarci in questi programmi di navigazione, ma le loro tecniche non funzionano nelle app, che sono immuni. Un esempio concreto: in questo periodo molti clienti di banche stanno ricevendo dei messaggi, via mail, SMS o WhatsApp, che li informano di una spedizione in arrivo e invitano a cliccare sul link per saperne di più. Ma si tratta di messaggi falsi, creati da truffatori; se si clicca sul link, tentano di installare sul computer o sul telefono una sorta di virus (più correttamente un "trojan", uno dei tanti periodicamente sfornati dai criminali informatici) che intercetta le comunicazioni bancarie, rubando password e codici di sicurezza per poi saccheggiare i conti bancari. Se però si usa l'app bancaria, questo attacco fallisce completamente e i soldi restano al sicuro. Le app bancarie, infatti, creano un canale di comunicazione sicuro e diretto con la banca. Inoltre prevengono



un altro trucco preferito dei malviventi: creare dei siti che imitano visivamente e nel nome quelli delle banche reali e indurre le vittime a visitarli. Per esempio, al posto di www.lamiabanca.ch i ladri creano www.larniabanca.ch, contando sul fatto che molte vittime non noteranno che la m è stata imitata mettendo insieme una r e una n e immetteranno i propri codici di accesso nel sito falso dei truffatori, credendo che sia quello della loro banca. Con le app questa tecnica non funziona.

Un altro vantaggio importante delle app è che possono sfruttare i sensori di identità dei telefonini, ossia i lettori di impronte digitali o le telecamere di riconoscimento del volto, e quindi verificare che chi sta dando ordini bancari sia davvero il cliente. In caso di furto del telefono, il ladro non potrà imitare l'impronta o il volto del proprietario e quindi non riuscirà a entrare nel conto bancario. I computer normalmente non hanno questi sensori e quindi devono usare altri sistemi di verifica, che sono più vulnerabili. Le app offrono anche un altro servizio utile: possono allertare subito il cliente in caso di transazioni anomale e permettergli di intervenire in pochi istanti. Il sistema di allerta tradizionale, basato sui messaggi SMS, è invece lento, non consente interventi altrettanto rapidi e offre il fianco a falsi allarmi inviati da truffatori. Vale insomma la pena sopportare questo ennesimo cambiamento e installare l'app della propria banca. E se il telefonino proprio non fa per voi, chiedete alla vostra banca se offre un apparecchietto apposito, chiamato di solito lettore Photo-TAN, per gestire l'accesso sicuro al conto: più compatto di un telefonino, ha una piccola telecamera che si usa per inquadrare il mosaico a colori di sicurezza mostrato dal sito della banca ed estrarne un codice di sicurezza temporaneo, che si aggiunge ai codici abituali per offrire maggiore protezione. È un buon compromesso per chi non ama le app.

Consigli ACSI

- Assicuratevi di installare l'app della vostra banca e non una sua imitazione fraudolenta: il modo più semplice è farsi aiutare da un addetto allo sportello o andare sul sito della banca stessa, che ospita un collegamento diretto all'app.
- Se decidete di non usare l'app e di restare al sistema tradizionale, non cliccate mai su un link ricevuto per e-mail o SMS: potrebbe essere falso. Digitate invece a mano il nome del sito della vostra banca nella barra degli indirizzi del vostro programma di navigazione.
- Il sito ebas.ch offre molti consigli utili, in linguaggio chiaro, su come gestire conti bancari via computer, tablet e telefonini.

Paolo Attivissimo

Risparmio energetico, **l'informatica** fa la sua parte

Si parla tanto, in questo periodo, di iniziative per il risparmio energetico, soprattutto in campo elettrico, e circolano dicerie e titoli di giornali che parlano del costo energetico di una email, di uno scambio di foto o di una videoconferenza. Le intenzioni sono lodevoli, ma c'è il rischio di creare un clima di ansia e mortificazione che non ha una giustificazione reale e distrae da interventi che possono dare risultati molto più concreti. Infatti il consumo energetico legato a computer, tablet e telefonini sempre accesi e alla trasmissione di dati via Internet ha un peso molto modesto sui consumi complessivi di energia, anche se si tiene conto della corrente consumata dai grandi depositi di dati gestiti dagli operatori oltre che di quella consumata a livello domestico e negli uffici.

È vero che guardare un video su YouTube consuma più energia che guardare un video che si trova sul proprio computer perché impegna i centri di calcolo e le reti di telecomunicazioni, ed è impressionante pensare che in meno di un anno l'ascolto via Internet della canzone di grande successo *Despacito* ha consumato la stessa quantità di energia elettrica usata da Ciad, Guinea-Bissau, Somalia, Sierra Leone e Repubblica Centrafricana tutte insieme, come denota una recente ricerca dell'Università di Zurigo e del Gottlieb Duttweiler Institut commissionata da Swico e Swisscleantech. Ma normalmente si tratta comunque di consumi quasi trascurabili rispetto a quelli causati dagli altri apparecchi elettrici di casa: l'unica eccezione è costituita dai computer ad alte prestazioni per videogioco o per la produzione di bitcoin o altre criptovalute, che assorbono molta energia e restano accesi per ore. La stessa ricerca osserva che l'impatto ambientale di tutta la normale filiera dei servizi digitali si attesta intorno al 3%.

I dati più recenti dimostrano che gli apparati domestici più energivori sono quelli di condizionamento e riscaldamento elettrico, che rappresentano quasi la metà dei consumi complessivi; il resto è composto in grandissima parte dagli scaldabagno o boiler elettrici, da lavatrici e asciugatrici e dagli impianti di illuminazione. Sorprendentemente, frigoriferi, forni elettrici e lavastoviglie incidono relativamente poco sul bilancio totale, mentre le automobili elettriche sono troppo poche, per ora, per avere un effetto significativo sui consumi elettrici nazionali.

Possiamo insomma mandare le email senza ansie ed evitare di assillare i nostri figli perché guardano i video in streaming (anche perché quando guardiamo la TV digitale facciamo sostanzialmente la stessa cosa, senza rendercene conto). Conviene concentrarsi sulle altre utenze elettriche di casa: abbassare leggermente il riscaldamento o l'aria condizionata oppure sostituire questi impianti con apparati più moderni ed efficienti e far partire la lavastoviglie solo quando è piena fa una differenza di gran lunga maggiore di qualunque rinuncia a Internet, computer e telefonini.

Tuttavia qualcosina si può fare anche in campo informatico senza grandi disagi: spegnere completamente scanner, stampanti, monitor, dischi rigidi esterni tradizionali (non SSD), televisori, lettori DVD o Blu-ray e videogiochi quando non sono in uso contribuisce a ridurre i consumi senza infastidire. Ma è importante che si tratti di spegnimenti veri, non di semplici "standby" con la spia luminosa accesa, altrimenti il consumo persiste: lo si nota dal calore che continua a essere emanato.

Già spegnere il modem/router di accesso a Internet di notte o quando si è fuori casa equivale a spegnere una lampada da comodino che altrimenti starebbe accesa notte e giorno. Questo spegnimento vero si può semplificare collegando tutti gli apparecchi spegnibili alla stessa presa multipla dotata di interruttore: è sufficiente spegnere quel singolo interruttore per togliere corrente a tutti i dispositivi. E volendo si può mettere un temporizzatore sulla presa multipla, in modo che lo spegnimento e la riaccensione siano automatici.

Consigli ACSI

- I "salvaschermo", ossia le immagini mostrate dai monitor e dai televisori quando non sono in uso, non riducono il loro consumo di energia: per non consumare, il dispositivo deve essere proprio spento.
- Gli alimentatori di molti tablet, telefonini e computer consumano corrente anche quando hanno finito di caricare i rispettivi dispositivi. Se li sentite caldi, toglieteli dalla presa per ridurre i consumi.
- Se spegnete il vostro modem/router di notte o durante le assenze, tenete presente che potreste perdere anche l'uso della linea telefonica fissa qualora questa linea passi attraverso il dispositivo.

Truffe natalizie, fra influencer e maiali

Paolo Attivissimo

Si dice sempre che a Natale siamo tutti più buoni, ma quest'idea decisamente non vale per i criminali informatici su Internet. Il periodo natalizio è da sempre uno dei loro momenti prediletti per mettere a segno truffe di tutti i generi approfittando della foga delle compere e dei buoni sentimenti mal riposti.

Gira da parecchi mesi, ma si sta facendo ultimamente più diffusa, una truffa che colpisce soprattutto i giovani utenti di Instagram e WhatsApp: il criminale si finge un loro amico e chiede loro di "dare un voto" per aiutarlo a "diventare un influencer" oppure chiede di girargli un codice di sei cifre mandato per errore all'utente. Se l'utente cade nella trappola, il truffatore gli manda un messaggio che contiene un link che, se cliccato, porterà la vittima a un sito o a un'app che gli ruberà il profilo chiedendone le credenziali in modo ingannevole.

A quel punto il ladro contatterà la vittima e chiederà un riscatto per ridarle il controllo del profilo; il pagamento avverrà tramite criptovalute oppure acquistando carte prepagate di Apple, Google o altri grandi fornitori e mandando i loro numeri di serie al truffatore. La media delle richieste di riscatto nei casi che mi sono stati segnalati in Ticino è di circa 200 franchi: una cifra calibrata per essere sopportabile e disincentivare denunce e azioni legali.

Come sempre, la prevenzione è la cura migliore, per cui è opportuno informare chi usa questi social network di stare in guardia contro richieste di questo genere e bloccarle immediatamente. Se il danno è ormai fatto, si può tentare il recupero del profilo rivolgendosi alle pagine web informative di Instagram e WhatsApp, facilmente trovabili digitando in Google "recuperare account rubato" seguito dal nome del social network. Se questo approccio fallisce, conviene semplicemente creare un profilo nuovo, se possibile, e fare tesoro dell'esperienza. Negoziare con il criminale è altamente sconsigliabile: se vede che la vittima è disposta a pagare, chiederà altri soldi. Sui social network circolano inoltre annunci che promettono acquisti a prezzi stracciati e guadagni facili tramite investimenti in criptovalute: purtroppo sono quasi sempre truffe estremamente professionali, con tanto di finto sito elegante del "negozio" o della "banca". Sto seguendo casi nei quali la vittima è stata convinta a investire cifre importanti ed era certa di aver realizzato guadagni ingenti, ma il "conto corrente" sul quale apparivano quei guadagni era in realtà una finzione molto realistica creata dai truffatori: alla richiesta di incassare, i truffatori rispondevano sempre con qualche scusa. Anche a Natale, insomma, vale la regola che se un'offerta è troppo bella per essere vera, quasi sicuramente non è vera. Conviene stare sui negozi e sulle banche digitali di buona reputazione, meglio se nazionali, e non affidarsi a sconosciuti.

Quest'anno, inoltre, ha preso piede una truffa particolarmente crudele già a partire dal nome: viene chiamata "pig butchering", ossia "macellazione del maiale", perché è così che i criminali vedono le proprie vittime. I truffatori selezionano i propri bersagli usando le informazioni che trovano sui social network: età, situazione sentimentale, foto. Prediligono le persone che non hanno un partner e mostrano nelle fotografie un'età adulta e una disponibilità economica significativa (mostrando per esempio la loro auto, il loro abbigliamento o le immagini dei loro viaggi).

Una volta scelta la vittima, la circuiscono con il metodo ormai tristemente classico del "romance scam" o truffa sentimentale: intrecciano una lunga relazione a base di messaggi e foto, senza chiedere nulla di insolito, diventano conoscenti di lunga data e si conquistano la fiducia del bersaglio con parole affettuose e una presenza costante e piacevole. L'inganno scatta solo dopo settimane o mesi di corteggiamento, ma a differenza della truffa classica, nella quale il criminale finge di avere bisogno di soldi temporaneamente per tirarsi fuori da un guaio burocratico o di salute, nel pig butchering non c'è nessuna richiesta di denaro, e questo fa abbassare ancora di più le difese psicologiche della vittima.

Il truffatore, ormai diventato un conoscente di lunga data, "rivela" alla vittima di aver fatto un ottimo investimento in criptovalute e le propone di fare altrettanto, dandole tutte le istruzioni necessarie su come versare soldi per aprire un "conto". Ma l'investimento non esiste, e il "conto" è gestito dal truffatore o da suoi complici. Solo negli Stati Uniti, questo raggiro ha generato incassi per oltre 18 milioni di dollari, sottratti a oltre 200 vittime, molte delle quali hanno perso i risparmi di una vita. A Natale, oltre a essere più buoni, cerchiamo di essere anche più vigili, avvisando anche amici e familiari di queste truffe.

Consigli ACSI

- Riducete le informazioni personali che pubblicate sui social network: anche una semplice foto con un edificio famoso sullo sfondo e un numero di targa permette ai truffatori di sapere tutto di voi.
- Attivate la cosiddetta "autenticazione a due fattori" sui vostri profili social e sulla vostra mail (le istruzioni si trovano digitando quest'espressione in Google). Questo "antifurto digitale" rende molto più difficile il furto dei profili.
- Se possibile, usate un computer o almeno un tablet per qualunque transazione su Internet che riguardi soldi: gli schermi grandi di questi dispositivi contengono più informazioni rispetto ai telefonini e aiutano a riconoscere eventuali siti truffaldini o ingannevoli.