



Difendersi dalle truffe online

Descrizione

In occasione della World investor week l'attissimo Museo del Risparmio di Torino si è occupato dell'attuale problema della cyber security. Se è vero che la tecnologia è abilitante e pur vero che la sola formazione e informazione aiutano a beneficiarne in sicurezza. La platea virtuale è stata coinvolta tramite sondaggi a verificare le proprie conoscenze e, ovviamente, ad aumentarle con la tecnica del commento delle risposte.

Dove l'evoluzione tecnologica non ha ancora portato dei cambiamenti? La risposta si è focalizzata per la maggiore proprio sull'identità fisica della persona, la quale la tecnologia affianca l'identità digitale della persona, generatrice di informazioni e modificabile. In quale percentuale l'errore umano influisce sulla sicurezza informatica? Per il 30,50, 70 o 90%? Pochi hanno davvero contezza di questo dato verificato statisticamente oltre la soglia del 90%: l'errore umano comporta il più alto rischio informatico. e questo addosso ad ognuno di noi una grande responsabilità.

Quante persone sanno esattamente definire il concetto di ingegneria sociale? Esso è insieme di tecniche volte a capire le informazioni sulla nostra identità digitale, da parte di hacker e cybercriminali che, fingendosi enti leciti, sono caratterizzati dall'aver un unico scopo in comune: trarre illecito profitto. In ogni occasione con ogni mezzo utile talvolta anche banale sniffano questo il termine tecnico usato in gergo – i nostri dati personali per usi illeciti, dannosi per le vittime profittevoli per loro.

Tra il phishing e lo smishing ed il calling quale è il più usato attualmente? Certamente il phishing il più atavico, usato già nell'ambito delle Poste e Telegrafi nei tempi passati: il costo è basso i risultati in genere ci sono. Tuttavia sta prendendo piede anche lo smishing, che utilizza la tecnica della messaggistica tramite lo smartphone. La tecnica della calling ovvero della telefonata è stata usata da truffatori informatici che utilizzano le persuasioni, spacciandosi per enti legali, riuscendo a mascherare anche il numero di chiamata reale con il numero corretto dell'ente e cercando di carpire le credenziali per lo più paventando la situazione di calinga urgenza, tale da indurre in agitazione preoccupazione la vittima.

Come fare a riconoscere queste situazioni e difendersi? La risposta la risposta è molta attenzione e

precauzione. verificare sempre la correttezza dell'URL, digitandolo direttamente, non cliccare sul link proposti non scaricare applicazioni se non dei siti ufficiali, non comunicare mai le proprie credenziali se non si è certi della legalità del nostro interlocutore e non cadere nella trappola dell'urgenza, senza le dovute verifiche. Fare sempre attenzione ai dettagli, gli allegati strani, gli errori grammaticali, anche se la grafica dei siti truffatori è sempre molto simile a quella dei siti legali.

E per quanto riguarda la password? Si è a conoscenza dei requisiti di sicurezza? Gli esperti elencano almeno sei requisiti: in primis la diversità per ogni account, lunghezza almeno 8 caratteri e la tipologia diversa di caratteri (numeriche, alfabetiche e speciale), il non uso di nomi comuni – molti hacker usano i vocabolari – ovvero di date o luoghi per noi significativi che si possono carpire dei dati sui social, riservatezza con frequenti aggiornamenti, almeno ogni 60 giorni ed infine la custodia sicura. Dove può essere il luogo sicuro per costruire custodire la nostra password? Ognuno di noi ha il proprio criterio, ma volendo si possono identificare in assoluto luoghi meno sicuri: il proprio smartphone sotto la voce password ovvero il foglietto del proprio portafoglio. Se è possibile, e consigliabile anche aggiungere livelli in più di protezione inserendo multi fattori di autenticazione, quali dati biometrici come l'impronta digitale o riconoscimento dei lineamenti del viso. E se si volesse controllare la robustezza della propria password? Anche qui la tecnologia viene in aiuto sul sito kaspersky.com e possibile farlo, ovviamente consigliando di non mettere la personale, ma una con caratteristiche analoghe per lunghezza e tipologia appunto. È anche possibile, grazie alla tecnologia verificare se si è stati coinvolti in incidenti informatici, magari a nostra insaputa e se è ovviamente correre ripari con le variazioni del caso.

Sotto l'aspetto più prettamente accademico il professore Michele Colajanni, ordine di ingegneria informatica presso l'università di Bologna e fondatore dell'accademia di cybersecurity, che, intervistato dalla del Museo del risparmio Giovanna paladino, puntualizza importanti e interessanti aspetti. Del resto, la pandemia acutizzato certe problematiche legate al mondo digitale, considerato che, come dicono i filosofi, ora siamo tutti "online", vivendo praticamente in connessione continua.

Purtroppo, un primo aspetto negativo: i giovani, in generale, non hanno contezza le esigenze di protezione dei propri dati personali, avendo altre priorità. La visibilità è un valore più alto rispetto alla privacy. Il valore dei like è fondamentale per la loro identità come persone, salvo poi pentirsene in futuro, non realizzano immediatamente che le loro stupidaggini non verranno dimenticate – come invece succede in tempi passati – dal web ma conservate a futura memoria. Del resto anche la giovane generazione di informatici preparatissimo in materia, non si rende bene conto dei rischi attuali per le persone medie: alcune loro conoscenze che mettono al riparo dai rischi informatici vengono date per scontate, ma non ci si rende conto di ingenuità dell'utenza media che non possiede la loro competenza.

Un punto sensibile da toccare quello delle donne nell'informatica perché sono ancora così poche? La società digitale ancora in formazione con regole da stabilire e vi è bisogno anche il contributo femminile della sensibilità, della curiosità intellettuale delle donne per evitare i problemi le battaglie che si sono verificate in passato nella società civile per il loro accesso a determinate professioni. Non si dimentichi che l'informatica offre ottime opportunità di lavoro, al momento la domanda supera l'offerta, che le competenze professionali permettono di scegliere il lavoro migliore.

Qual è il messaggio finale che si può trarre? Alla sicurezza informatica con l'investimento che essa comporta deve essere un valore che i consumatori devono pretendere dei prodotti dispositivi informatici, al di là e al di sopra del design delle funzionalità. Sul versante comportamentale, che come si è detto una forte rilevanza sui rischi informatici, è necessario prestare molta attenzione nell'uso. Così come si fa attenzione ad attraversare la strada e a guidare un'auto, si deve prestare attenzione all'uso, anche domestico, dei dispositivi informatici che possono rivelarsi molto pericolosi. Ma il pericolo fisico è atavico e quindi cognitivamente meglio elaborato. Questo pericolo invece una nuova dimensione, più labile e più insidiosa in quanto meno tangibile. È necessario in questo campo una buona educazione per il corretto e sicuro uso della tecnologia informatica sempre più avanzata. Il prossimo orizzonte potrebbe essere proprio quello di implementare corsi online di cyber security non solo per i professionisti ma anche per autodifesa e igiene digitale.

Liliana Perrone

CATEGORY

1. Innovazioni

Categoria

1. Innovazioni

Data di creazione

21/10/2021

Autore

perrone

default watermark