Difendersi dalle truffe online

Descrizione

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

Dove lâ€™evoluzione tecnologica non ha ancora portato dei cambiamenti? La risposta si Ã¨ focalizzata per la maggiore proprio sullâ€™identitÃ fisica della persona, la quale la tecnologia perÃ² affiancato lâ€™identitÃ digitale della persona, generatrice di informazioni e modificabile. In quale percentuale lâ€™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%: lâ€™errore umano comporta il piÃ¹ alto rischio informatico. e questo addosso ad ognuno di noi una grande responsabilitÃ .

Quante persone sanno esattamente definire il concetto di ingegneria sociale? Esso lâ€™insieme di tecniche volte a capire le informazioni sulla nostra identitÃ digitale, da parte di hacker e cybercriminali che, fingendosi enti leciti, sono caratterizzati dallâ€™avere un unico scopo in comune: trarre illecito profitto. In ogni occasione con ogni mezzo utile talvolta anche banale sniffano â€“ 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 Ã¨ il piÃ¹ usato attualmente? Certamente il phishing il piÃ¹ atavico, usato giÃ nellâ€™ambito delle Poste e Telegrafi nei tempi passati: il costo e 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 Ã¨ 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 dellâ€™ente e cercando di carpire le credenziali perlopiÃ¹ 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 Ã¨ molta attenzione e

precauzione. verificare sempre la correttezza dellâ€™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 Ã¨ piÃ¹ certi della legalitÃ del nostro interlocutore e non cadere nella trappola dellâ€™urgenza, senza le dovute verifiche. Fare sempre attenzione ai dettagli, gli allegati strani, gliele agli errori grammaticali, anche se la grafica dei siti truffatori Ã¨ sempre molto simile a quella dei siti legali.

E per quanto riguarda la password? Si Ã¨ a conoscenza dei requisiti di sicurezza? Gli esperti elencano almeno sei requisiti: in primis la diversitÃ 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 puÃ² 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 Ã¨ possibile, e consigliabile anche aggiungere livelli in piÃ¹ di protezione inserendo multi fattori di autenticazione, quali dati biometrici come lâ€™impronta digitale o riconoscimento dei lineamenti del viso. E se si volesse controllare la calinga robustezza della propria password? Anche qui la tecnologia viene in aiuto sul sito karspersky.com e possibile farlo, ovviamente consigliando di non mettere la personale, ma una con caratteristiche analoghe per lunghezza e tipologia appunto. Ãˆ anche possibile, grazie alla tecnologia verificare se si Ã¨ stati coinvolti in incidenti informatici, magari a nostra insaputa e se sÃ¬ ovviamente correre ripari con le variazioni del caso.

Sotto lâ€™aspetto piÃ¹ prettamente accademico il professore Michele Colajanni, ordine di ingegneria informatica presso lâ€™universitÃ di Bologna e fondatore dellâ€™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 â€œon lifeâ€•, 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 prioritÃ . La visibilitÃ Ã¨ un valore piÃ¹ alto rispetto alla privacy. Il valore dei like Ã¨ fondamentale per la loro identitÃ come persone, salvo poi pentirsene in futuro, non realizzano lâ€™immediato 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 ingenuitÃ dellâ€™utenza media che non possiede la loro competenza.

Un punto sensibile da toccare quello delle donne nellâ€™informatica perchÃ© sono ancora cosÃ¬ poche? La societÃ digitale ancora in formazione con regole da stabilire e vi Ã¨ bisogno anche il contributo femminile della sensibilitÃ , della curiositÃ intellettuale delle donne per evitare i problemi le battaglie che si sono verificate in passato nella societÃ civile per il loro accesso a determinate professioni. Non si dimentichi che lâ€™informatica offre ottime opportunitÃ di lavoro, al momento la domanda supera lâ€™offerta, che le competenze professionali permettono di scegliere il lavoro migliore.

Â Qual Ã¨ il messaggio finale che si puÃ² trarre? Alla sicurezza informatica con lâ€™investimento che essa comporta deve essere un valore che i consumatori devono pretendere dei prodotti dispositivi informatici, al di lÃ e al di sopra del design delle funzionalitÃ . Sul versante comportamentale, che come si Ã¨ detto una forte rilevanza sui rischi informatici, Ã¨ necessario prestare molta attenzione nellâ€™uso. CosÃ¬ come si fa attenzione ad attraversare la strada e a guidare lâ€™auto, si deve prestare attenzione allâ€™uso, anche domestico, dei dispositivi informatici che possono rivelarsi molto pericolosi. Ma il pericolo fisico Ã¨ atavico e quindi cognitivamente meglio elaborato. Questo pericolo invece una nuova dimensione, piÃ¹ labile piÃ¹ insidiosa in quanto meno tangibile. Ã^ necessario in questo campo una buona educazione per il corretto e sicuro uso della tecnologia informatica sempre piÃ¹ 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