Comunicare in sicurezza
Bologna 2 dicembre 2021
Ore 15.30

Relatore

Adriana Apicella

Direttore Generale CONFASSOCIAZIONI

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

Comunicazione del rischio = scambio interattivo tra individui (o gruppi di individui) dove bisogna privilegiare l'informazione corretta senza creare allarmismi.

Come fare per migliorare la posizione, poco agevole, di chi comunica potenziali pericoli attraverso un elenco di dati e analisi scientifiche o, cosa ricorrente in questo periodo, epidemiologiche?

Ecco alcuni punti essenziali:

- Considerare le ripercussioni emotive e psicologiche di chi ascolta. L'uomo è come un iceberg dove la parte emergente è rappresentata anche dai comportamenti e la parte restante è fatta di motivazioni, atteggiamenti, valori e principi. I comportamenti umani sono, quindi, determinati o influenzati da cause non visibili in superficie e a volte addirittura sconosciute al soggetto in azione.
- Essere chiari nell'esposizione ma non freddi
- Mettersi in ascolto
- Coinvolgere gli uditori

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

Saper comunicare vuol dire assumersi la responsabilità di quanto succede, senza dare le colpe ad altre persone, altre situazioni, altri momenti, ma piuttosto analizzare la propria comunicazione (verbale e non verbale) così da individuare il gap che ha determinato una comunicazione non idonea alla circostanza.

I nostri successi dipendono da come comunichiamo: è fondamentale adattare le parole e l'atteggiamento adeguato alla situazione affinché l'altro possa comprendere nel profondo e, perché no, toccare la parte emotiva facendogli battere il cuore

La tigre e la neve, regia Roberto Benigni, 2005

https://www.youtube.com/watch?v=NXTmJWmqL1U

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

Nella vita sono tantissime le persone che si preoccupano di chi (o di che cosa) abbia procurato il dolo per poi incolparlo, molto meno quelle che agiscono per raggiungere il risultato positivo. Ovvero più persone orientate al problema che persone orientate alla soluzione.

Più che rimuginare sull'episodio, per ore intere, a volte per mesi o anni - la qual cosa peggiora e rinforza il problema - bisogna essere orientati alla soluzione.

Perché, come si domandava Richard Bandler, «*se cadi in un fiume, sei più interessato a sapere come venirne fuori, oppure a scoprire perché ci sei caduto?*»

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

Sicuramente come in un qualsiasi processo di comunicazione anche per quello relativo alla comunicazione del rischio è necessario investire, soprattutto nella fase iniziale, la giusta energia per creare un rapporto di fiducia tra il lavoratore e il comunicatore del rischio.

In tal modo si motiva la sicurezza in modo duraturo, si diffonde la visione della sicurezza come scelta aziendale e si trasforma la sicurezza stessa da un processo obbligatorio a un processo lavorativo qualitativamente alto fatto di migliori relazioni interpersonali, di atteggiamenti proattivi e spontanei dei lavoratori e di azioni preventive agli infortuni e alle situazioni rischiose.

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

"Il Web non è diverso dall'umanità,

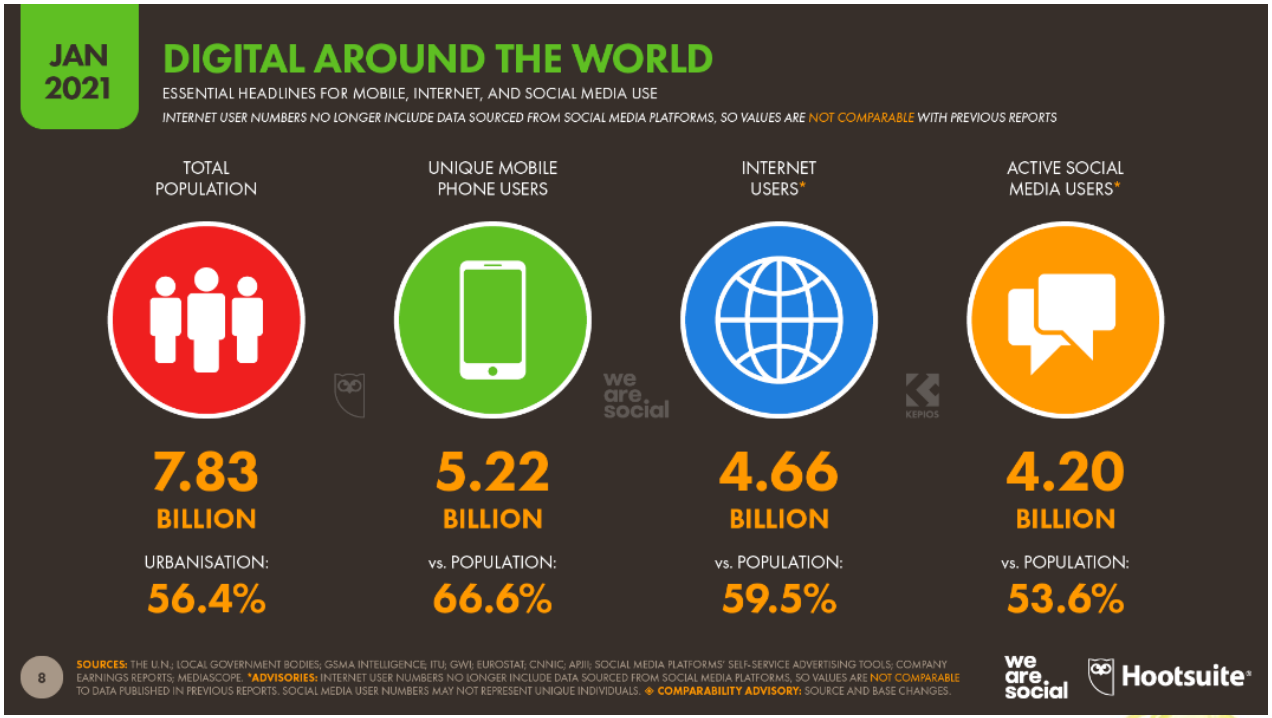
che è fatta di cose **orribili** e altre **meravigliose**.
Chi accusa il Web di avere un lato **oscuro**,
dovrebbe **riflettere** sul fatto che quel lato oscuro è nell'umanità stessa.
Ciò detto io sono **ottimista** e resto convinto che il saldo **finale**,
il bilancio di una umanità più **connessa** resta positivo".

Tim Berners-Lee

Disconnect, regia di Henry-Alex Rubin, 2014

https://www.youtube.com/watch?v=z6WoQJfHRM4&t=1s

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

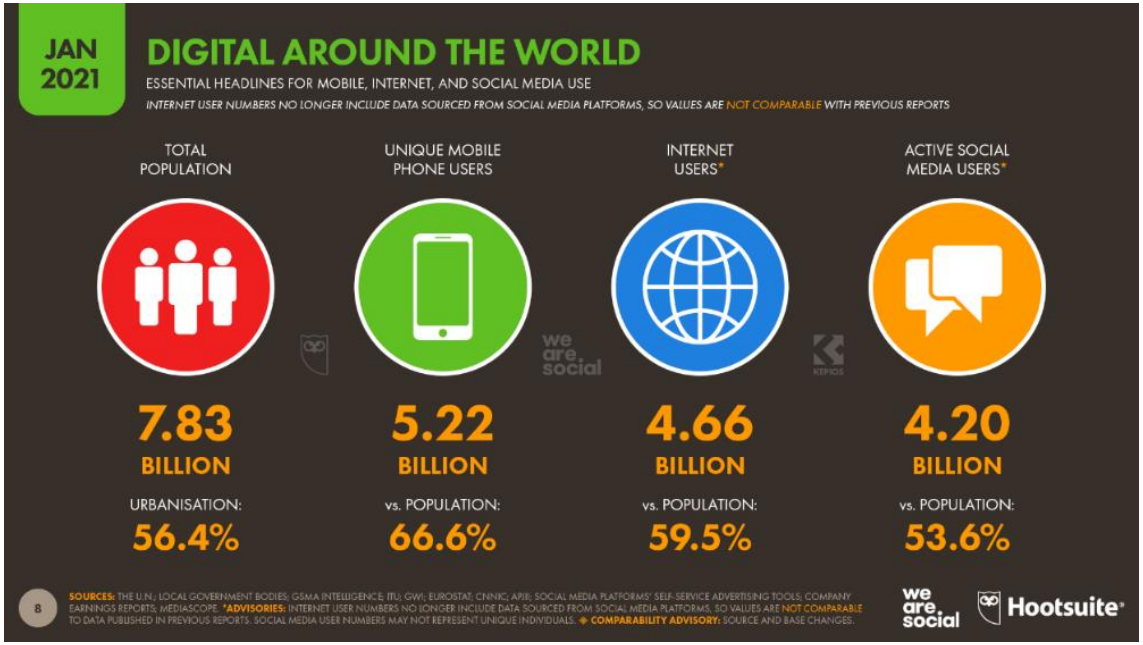


La rete: qualche numero

Ad inizio del 2021 abbiamo raggiunto i **7,83 miliardi** di persone nel mondo con un tasso di crescita dell'1% annuo. Questo indica che nel corso del 2020 siamo cresciuti di circa **80 milioni** di unità (fonte Nazioni Unite)

Fonte: Digital 2020 we are social & Hootsuite

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI



Di questi 7,83 miliardi di persone:

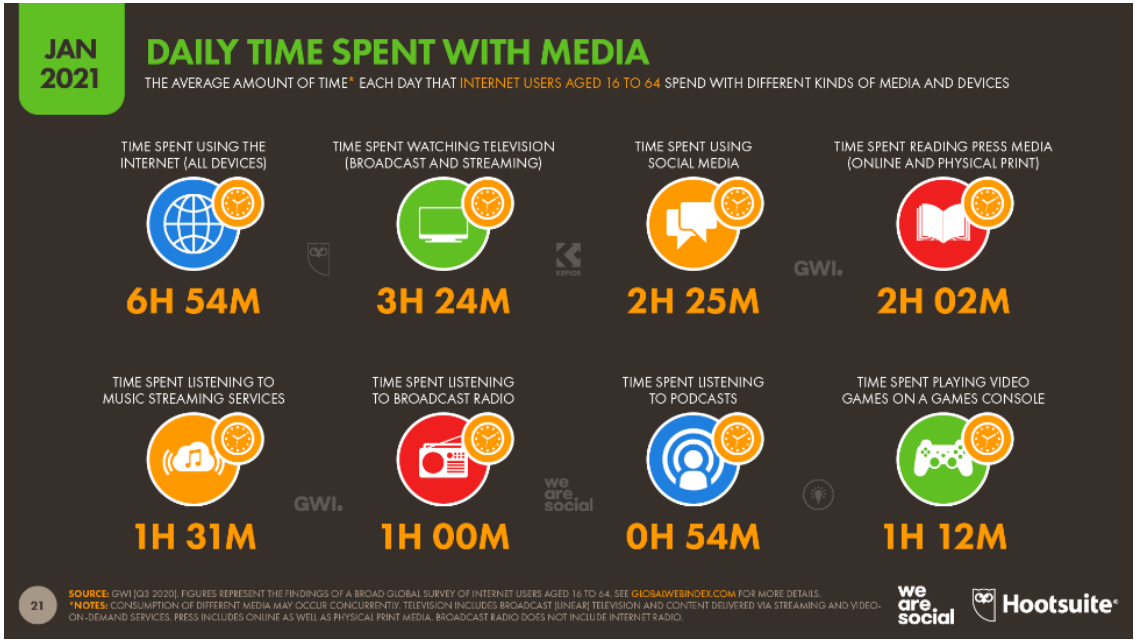
5,22 miliardi utilizzano telefoni cellulari (ovvero il **66,6%** della popolazione). Inoltre nel corso del 2020 hanno avuto accesso ad un telefono cellulare per la prima volta 93 milioni di persone (l'1,8% su base annua).

4,66 miliardi accedono ad internet: un incremento del **7,3%** (o di **316 milioni di persone**) rispetto a Gennaio 2020. La penetrazione internet mondiale si attesta al **59,5%.**

4,20 miliardi sono gli utenti delle piattaforme social: un incremento del **13%**, (o di **490 milioni** di persone che significa **oltre 1,3 milioni di persone ogni giorno**, o **15 persone al secondo**). La penetrazione delle piattaforme social si attesta al **53%** della popolazione mondiale.

Fonte: Digital 2020 we are social & Hootsuite

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI



Continua a crescere il tempo trascorso sulle piattaforme social anche se in misura più contenuta rispetto agli ultimi anni. Infatti si attesta a 2 ore e 25 minuti al giorno, che equivale a quasi un giorno intero alla settimana.

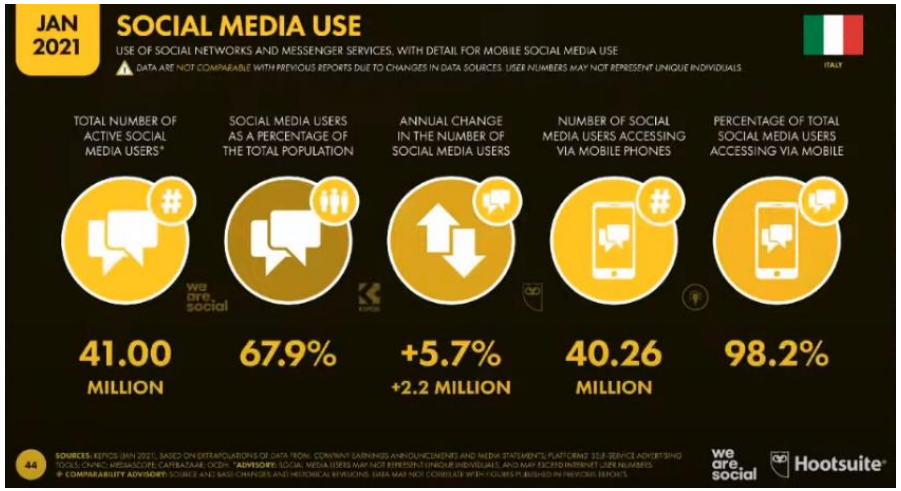
Se continua così, nel corso di quest'anno, saranno 420 milioni gli anni trascorsi su queste piattaforme.

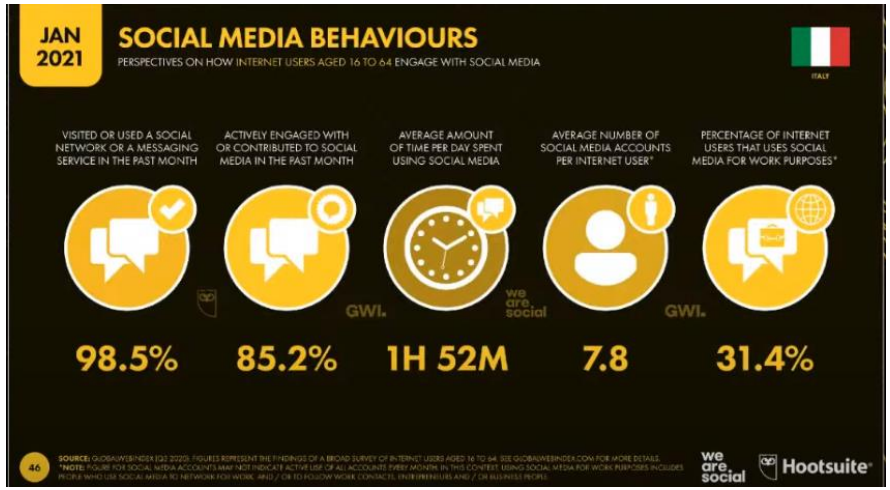
Riguardo il mondo più ampio della rete, l'utente medio passa online circa **7 ore al giorno**, vale a dire circa il 42% del tempo di veglia se si considera un riposo di 7-8 ore.

Si tratta di **un aumento di oltre un quarto d'ora al giorno** rispetto alla rilevazione di 12 mesi fa, o del 4% che, se mantenuto, porterebbe il tempo totale online speso da tutti noi a **1,3 miliardi di anni**.

Fonte: Digital 2020 we are social & Hootsuite

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI





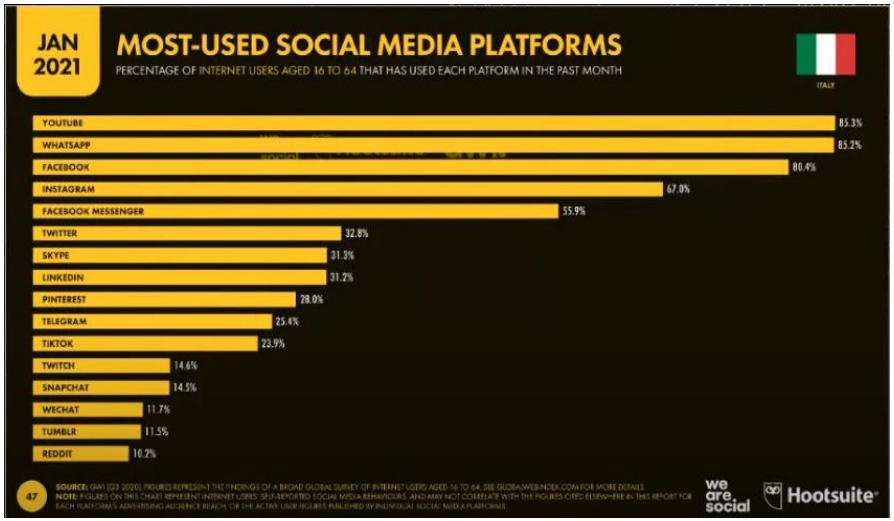
Italia

Siamo sempre più social e quasi tutti da mobile: a febbraio di quest'anno si contavano già oltre due milioni di persone connesse per la prima volta dall'inizio dell'anno.

Siamo sempre più partecipativi: i dati rilevano che l'85% degli italiani connessi ha partecipato a conversazioni sui canali social (con un aumento in punti percentuale del 4% rispetto allo scorso anno). Mediamente sono 8 le piattaforme più utilizzate.

Fonte: Digital 2020 we are social & Hootsuite

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI



Avanzano Telegram e TikTok, mentre su YouTube sono oltre 500 le ore di video che vengono caricate ogni minuto e oltre il miliardo le ore di video guardati ogni giorno.

E infine, l'uso degli smartphone ha raggiunto livelli di saturazione. Infatti già lo scorso anno la connessione da dispositivi mobili superava il 98% (dato quantitativo). A questo si aggiunge il contributo al dialogo degli utenti, e quindi il loro coinvolgimento, che tra il 2019 e il 2020 è salito dal 74% all' 81% (dato qualitativo).

Questo dialogo in rete non sempre è costruttivo o positivo ma può dar vita anche a fenomeni di disinformazione (nel 2020 le fake news si sono più che triplicate) o di errato comportamento.

Fonte: Digital 2020 we are social & Hootsuite

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Le fake news hanno una forte potenza mediatica e viaggiano così velocemente da influenzare l'opinione pubblica attraverso le piattaforme social.

L'interazione continua con persone con cui andiamo d'accordo e la proposta di contenuti che potrebbero interessarci da parte degli algoritmi di AI determinano la "bolla dei Social Media": finiamo col credere a quella cosa facilmente, senza cercare di capire se è vera o meno.

Siamo entrati così in una eco chamber (camera dell'eco), un meccanismo cognitivo che può portare alla disinformazione online (e quindi alla viralizzazione delle fake news).

Questo atteggiamento ripetuto vanifica l'azione positiva della rete e dei social media che è quella di offrire l'opportunità di comunicare per confermare o dissentire socialmente, politicamente e culturalmente.

È fondamentale, quindi, essere consapevoli, critici e creativi nell'uso della rete per non ledere la libertà/sensibilità/sicurezza delle altre persone.

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Come fare a capire se si tratta di una fake news

Assicurarsi che la notizia sia scritta da una fonte la cui reputazione sia attendibile. Se mancano prove o riferimenti a esperti senza nome, la notizia è falsa.

Non fidarsi dei titoli: le notizie false spesso hanno volutamente dei titoli altisonanti scritti in maiuscolo e con ampio uso di punti esclamativi.

Confrontare bene la URL. Se l'indirizzo web è molto simile a quello di una fonte attendibile potrebbe indicare che la notizia è falsa. In questo modo molti siti di notizie false si fingono autentici.

Attenzione alla formattazione: impaginazione strana o testo con errori di battitura.

Verificare le foto perché le notizie false spesso contengono immagini e video ritoccati, oppure autentici, ma presi da un altro contesto. È bene verificarne l'origine.

Controllare le date. Le date degli avvenimenti contenuti nelle notizie false potrebbero essere errate e la loro cronologia potrebbe non avere senso.

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Nel report di fine 2020 di Kaspersky "Story of the year: remote work", rispetto al 2019, in Italia, è stata registrata una crescita del 280% degli attacchi di forza bruta sui protocolli RDP (Remote Desktop Protocol) per un totale di 174 miliardi di file dannosi mascherati da applicazioni di comunicazione aziendale.

Gli anelli deboli sono stati i dipendenti che hanno iniziato a lavorare in smart working, le aziende non preparate a questa nuova modalità e coloro che hanno iniziato a utilizzare strumenti di comunicazione online e servizi di acquisto online.

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Sempre nel 2020 si è registrato un aumento di attacchi diretti al patrimonio personale dei cittadini, al tessuto economico-produttivo del Paese, alla regolarità dei servizi pubblici essenziali, al mondo delle professioni fino alla sicurezza e alla libertà personale di adulti e ragazzi.

Il Centro Nazionale Anticrimine Informatico per la protezione delle infrastrutture critiche ha rilevato una crescita del 246% degli attacchi alle infrastrutture critiche rispetto all'anno precedente.

Le transazioni fraudolente sul web sono state 744 per un totale di circa 9 milioni di euro, la Polizia postale ha rilevato un incremento di false raccolte sul web, sull'onda emotiva del supporto alla lotta covid-19, trattando complessivamente 93.300 casi e sottoponendo ad indagine 3.860 persone

Non mancano le truffe online in pole position anche a causa della paura scatenata dalla pandemia attraverso la tecnica più usata che è il pishing

Fonte: Rapporto 2021 Clusit (Associazione Italiana per la Sicurezza Informatica)

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete_Il Pishing

Il phishing punta a pescare i dati finanziari, quelli personali e le credenziali bancarie degli utenti della Rete. Si presenta attraverso una email che solo in apparenza è stata inviata da banche o istituti di credito (o altre enti accreditabili).

Solitamente, per rassicurare l'utente, nel messaggio c'è un link che rimanda - solo in apparenza - al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato abilmente allestito come quello originale. Se si cade nel tranello, una volta inseriti i propri dati riservati, questi finiranno nella mani di criminali informatici.

Che cosa fare? Diffidare da tutte quelle e-mail che chiedono dati personali (codice utente e password dei servizi bancari), utilizzano toni intimidatori (ad es: possibile blocco del conto corrente), contengono errori grammaticali, contengono link che portano a siti ingannevoli, hanno una url non protetta o contengono caratteri poco coerenti con il resto.

Mai inserire dati personali, non scaricare e aprire allegati che vi sono contenuti ma buttare subito la mail sospetta e svuotare il cestino.

In caso di truffa cambiare subito le credenziali dei siti collegati alla truffa (username e password) e nel caso di conti correnti bancari contattare subito la banca (da sentire anche in caso di msg telefonici o su whatsApp sospetti) e sporgere denuncia alla Polizia Postale.

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Il Pishing

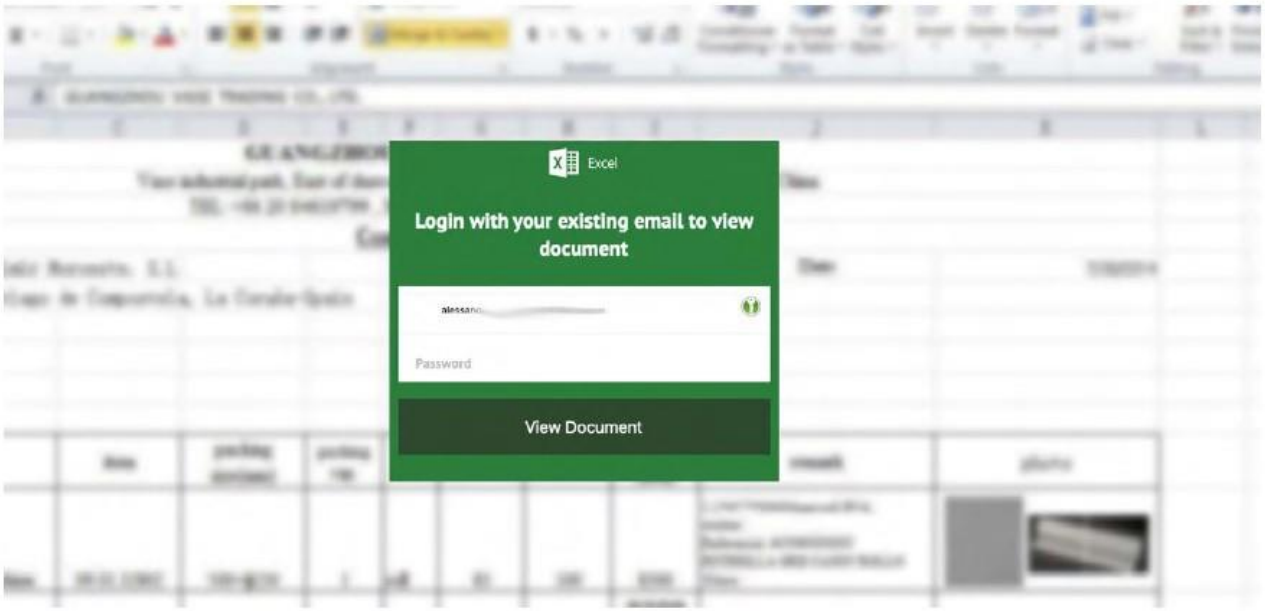


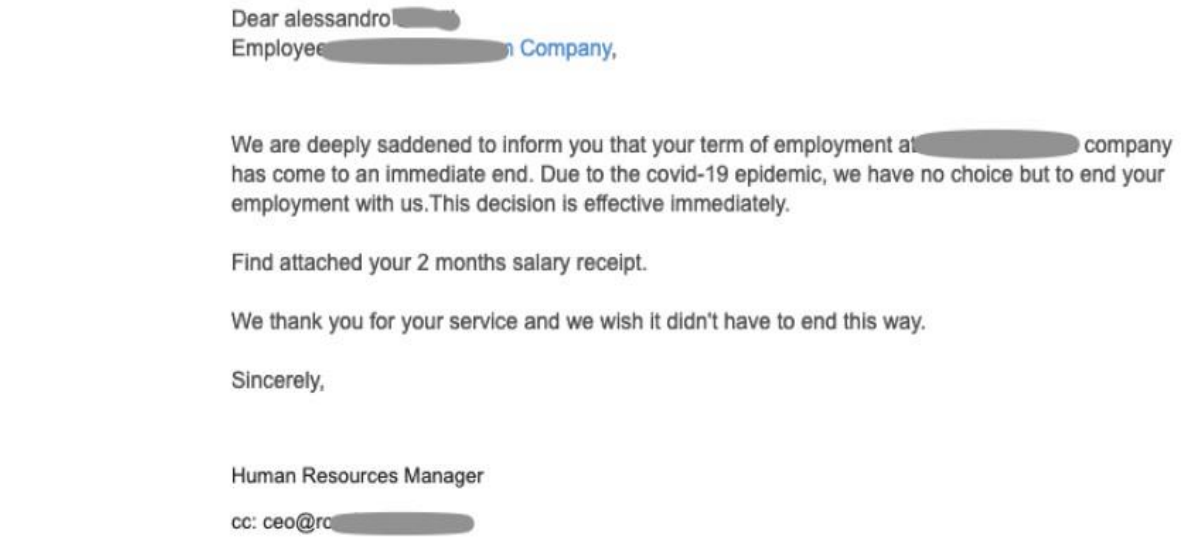
Figura 4 - *Allegato malevolo per carpire credenziali. Fonte: Libraesva*

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Rapporto 2021 sulla Sicurezza ICT in Italia

Il Pishing



Dear alessandro
Employee n Company,

We are deeply saddened to inform you that your term of employment at company has come to an immediate end. Due to the covid-19 epidemic, we have no choice but to end your employment with us.This decision is effective immediately.

Find attached your 2 months salary receipt.

We thank you for your service and we wish it didn't have to end this way.

Sincerely,

Human Resources Manager

cc: ceo@ro

Figura 3 - *Campagna di phishing, finto licenziamento causa COVID. Fonte: Libraesva*

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Il Pishing


Mondiale della Sanita - Italia

From: super <gestione@servicook.com>

To:

Date: Fri, 25/09/2020 12:12

documento_57.xls

Sha256: e4e3343985fb6e8d82efbfe631cd88ee47cfca7de2b3bdfc45b1da64ee4ea209

208.50 KB

Spett. Azienda

A causa del fatto che nella sua zona sono affermati casi di infezione da Coronavirus, l'Organizzazione Mondiale della Sanità ha messo a disposizione un documento che include tutte le prudenze necessarie contro l'infezione da Coronavirus. Le consigliamo quindi di leggere il documento incluso in questa mail.

Password : coronavirus

Cordiali Saluti,
Roberta Sirtari (Organizzazione Mondiale della Sanità - Italia)

Figura 6 - *Campagna di phishing che si spaccia per OMS. Fonte: Libraesva*

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Il Pishing

Panoramica dei cyber attacchi più significativi del 2020 e tendenze per il 2021


Progetto riapertura parziale dell' attivita economica ai fini della ripartenza dell'economia: indicazioni per le attivita

From: conferma <super@economicoppo.casa>
To:
Date: Tue, 17/11/2020 01:55

sviluppo_economico_11_139.zip
Sha256: 02daac8c4efb72e720fca1836c6c31fcdfa9a2771ee1089af1223d0313d1f1fe
52.01 KB

MEF Ministero dell'Economia e delle Finanze

Oggetto: Progetto riapertura graduale dell'attivita commerciale e produttiva ai fini della ripartenza dell'economia: indicazioni per le attivita

Il ministro dell'economia e delle finanze;

DISPONE URGENTEMENTE ai titolari d'impresa di verificare mediante l'archivio allegato a questa email le ultime modifiche effettuate alle ordinanze e l'eventuale corrispondenza della loro categoria di attivita all'interno dei nuovi elenchi di attivita limitate , ed eventuali modalita associate, allo scopo di gestire le riaperture con un ragionevole anticipo.

(Disposizioni finali)
Le disposizioni del presente decreto producono effetto in data 20/11/2020

Roma, ""17/11/2020""

Figura 7 - *Campagna di phishing che si spaccia per il MEF. Fonte: Libraesva*

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

1 **Cyberbullismo**
Attacco virtuale per intimorire, molestare, mettere in imbarazzo o semplicemente far sentire a disagio altre persone. Pettegolezzi, immagini o video imbarazzanti, costruzione di falsi profili social sono solo alcune delle modalità con cui possono essere realizzati gli attacchi online con finalità di cyberbullismo.

2 **Cybermolestie**
Comportamenti indesiderati e molestie attuate tramite Internet e i social network.

3 **Cyberstalking**
Comportamenti persecutori commessi mediante l'utilizzo del web. L'utilizzo della rete comporta infatti l'immissione online di numerosi dati personali che possono essere facilmente reperiti e utilizzati dallo stalker.

4 **Phishing**
È un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi una persona o un ente affidabile in una comunicazione digitale.

5 **Body shaming**
Commenti, video offensivi, denigrazioni che hanno come argomento il corpo del soggetto che si vuole colpire. Si mettono in evidenza in maniera denigratoria difetti fisici, abbigliamento e abitudini dell'alimentazione.

6 **Adescamento, violenze sessuali online, sexting, sextortion**
I minori in questo caso sono sottoposti attraverso la rete ad episodi di violenza a sfondo sessuale, che si traducono spesso nell'uso di un linguaggio spinto fino a arrivare all'adescamento dei minori da parte di soggetti adulti. In questo caso spesso vengono condivise immagini e video a sfondo pedopornografico.

7 **Uso incontrollato dei dati personali**
In questo caso i dati dei minori possono essere usati per la creazione di un alter ego digitale (Impersonation), per una sostituzione di persona (Masquerade) oppure si può utilizzare un'identità fittizia per conquistare la fiducia di un minore e poi aggirarlo (Trickery).

8

Fonte: Guida a cura di Società Italiana di Pediatria, la Polizia postale, Google, A.N.C.I. e UniCredit Foundation

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete

Fonte: Guida a cura di Società Italiana di Pediatria, la Polizia postale, Google, A.N.C.I. e UniCredit Foundation

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete_Cosa fare?

Anche per il mondo virtuale - per far comprendere bene i rischi che si celano in azioni di quotidiana routine - è necessario comunicare costantemente e ampiamente il rischio, con un linguaggio meno tecnico e diffuso tra i diversi target (in primis nelle scuole anche primarie dove argomenti come l'uso della rete, consapevolezza, conoscenza delle opportunità e dei rischi devono far parte del bagaglio di conoscenze al pari dell'italiano e della matematica). Solo attraverso campagne mirate e una buona formazione si può creare cyber consapevolezza nei cittadini, nei lavoratori, nelle imprese.

Fonte: Rapporto 2021 Clusit (Associazione Italiana per la Sicurezza Informatica)

Comunicare in sicurezza - Adriana Apicella, DG CONFASSOCIAZIONI

I rischi nella rete_Cosa fare per creare un rapporto di fiducia in rete?

- Rispetta il principio della youtility (renditi utile) e della reciprocità (regala valore).
- La trasparenza deve essere una prerogativa. Essere sinceri e diretti ripaga sempre. È nocivo dare informazioni che non corrispondono al vero solo per attirare l'attenzione. Quest'azione può avere un effetto boomerang. Dalla trasparenza alla fiducia il passo è breve: rivelarsi una fonte attendibile fa crescere in reputazione rendendovi un punto di riferimento.
- Quando proponi un argomento (ricorda la sicurezza è una delle 4 S dei bisogni primari dell'uomo, quindi spronare alla prevenzione non è così difficile come potrebbe sembrare) scrivi un testo semplice che anticipa la lettura. In sintesi qualche rigo che introduce e accompagna il contenuto di approfondimento.
- Mantieni alto il livello di serietà e professionalità e non cadere nella trappola della polemica sterile, evita le cadute di stile utilizzando il tono di chi attacca perché altrimenti rischi di intaccare il livello di reputazione aziendale (e personale) sia nella sfera reale che in quella virtuale (perché se è vero che ci vogliono anni per costruire una reputazione bastano pochi minuti in rete per distruggerla). Le due realtà camminano insieme perché l'una rafforza e sostiene l'altra.
- Di fronte alle critiche negative fai sempre domande, considerando lo stato d'animo dell'altro (e il perché ha detto determinate cose). In questo modo si smorzano i toni e si arriva a una soluzione pacifica. Muoviti, cioè, sull'onda dell'empatia e chiediti: che cosa pensa in questo momento l'altra persona? Quali sono le sue esigenze specifiche?