SMART WORKING VADEMECUM

CYBERSECURITY & SMART WORKING

CONSIGLI PRATICI PER SVOLGERE LE PROPRIE ATTIVITÀ LAVORATIVE DA CASA CON SERENITÀ E IN SICUREZZA

La situazione attuale ci costringe a rivedere le nostre abitudini, private e professionali; lo Smart Working ad esempio è diventato strumento essenziale per proseguire le attività aziendali, portandoci ad approcciare il lavoro in modo diverso rispetto a prima, con i suoi evidenti pro e contro.

Se da un lato questa condizione forzata ci permette di proteggerci dal pericolo sanitario, l'attività da casa non deve farci perdere di vista un aspetto molto importante per la salvaguardia del business della propria azienda in un periodo, per diversi aspetti, già estremamente delicato: la sicurezza informatica.

Non è un caso, infatti, che una serie piuttosto lunga di attacchi informatici abbia preso il via proprio in questo periodo, in cui tutti noi siamo particolarmente sensibili e a volte impreparati.

Molti di questi attacchi sfruttano proprio il tema "Covid-19" per aumentare di interesse ed essere quindi più efficaci.

CURIOSITÀ

A seguito del'allarme sanitario di questo periodo, sono stati registrati più di 13.000 domini con all'interno parole quali ad esempio "corona", "covid", "epidemia", "pandemia" etc.

Secondo voi saranno utilizzati tutti con scopi leciti?!

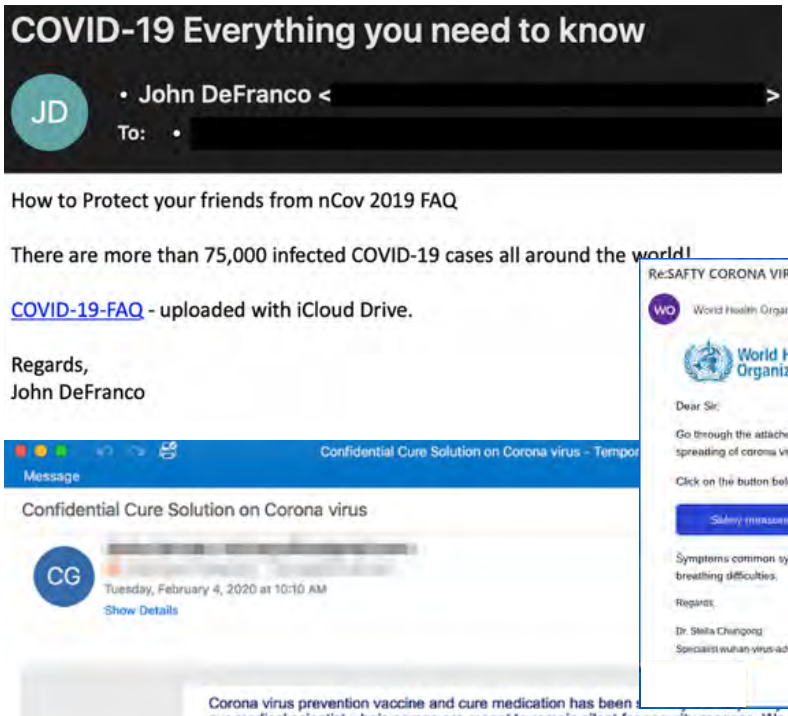
Mentre alcuni risultato legittimi, per altri invece è difficile sapere al momento il motivo per i quali sono stati creati. Per questo motivo è importante prestare estrema attenzione a tutte le comunicazioni relative al tema "coronavirus", in tutte le sue declinazioni, dando credito solamente a quelle che provengono dalle fonti ufficiali o delle quali riconosciamo inequivocabilmente l'origine come lecita.
Di seguito alcuni esempi di domini comprovati essere potenzialmente pericolosi perché utilizzati per finalità illegali:

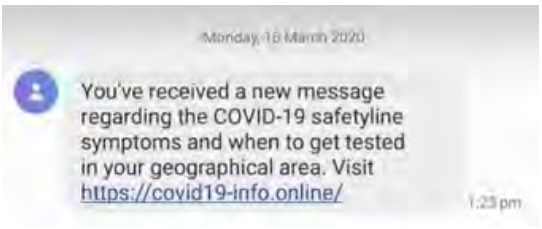
- coronavirusstatus.space
- coronavirus-map.com
- blogcoronacl.canalcero.digital
- coronavirus.zone
- coronavirus-realtime.com
- coronavirus.app

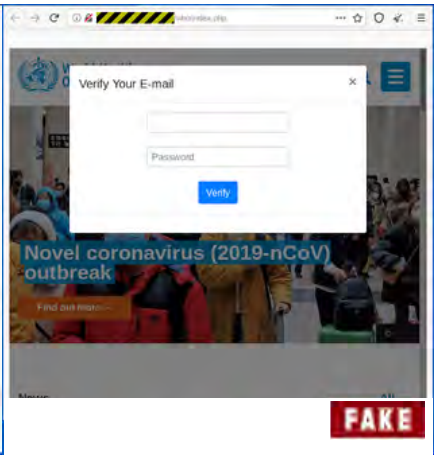
Perché in questo periodo siamo più vulnerabili alle minacce informatiche?

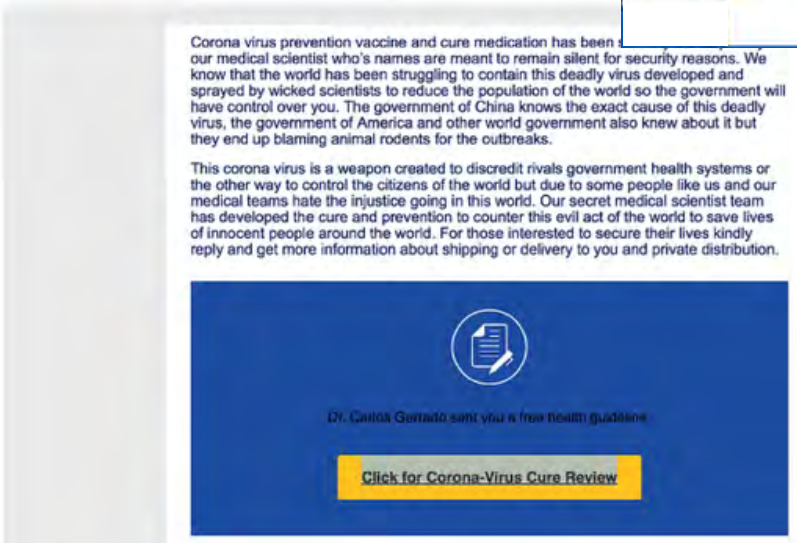
- Lavoriamo da casa, quindi non siamo coperti da normali presidi tecnologici che normalmente garantiscono la nostra protezione in ufficio.
- Siamo più isolati, non abbiamo colleghi con cui confrontarci se succede qualcosa di strano.
- In alcuni casi utilizziamo strumenti non aziendali, il PC di casa ad esempio.
- Può esserci la tentazione di "prestare" il PC aziendale ai nostri figli per ottenere qualche minuto di tregua.
- Siamo bombardati da notizie e aggiornamenti sul Covid19 che, in particolare, i più ansiosi di noi visualizzano senza accortezza.
- Le buone norme di comportamento acquisite in ufficio vengono disattese quando si lavora da casa (es. blocco del PC).

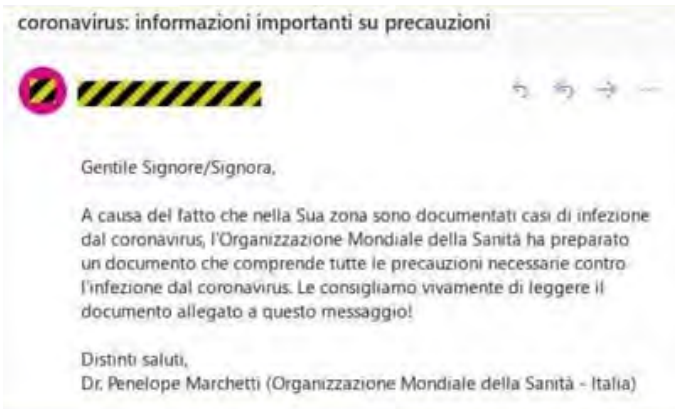
Queste "vulnerabilità" del nostro essere umani vengono sfruttate da malintenzionati attraverso vere e proprie campagne di phishing veicolate tramite e-mail, Whatsapp, Telegram ed i Social Network in generale. Di seguito alcuni esempi.











Bastano però alcuni semplici accorgimenti per svolgere le proprie attività lavorative da casa con serenità. Di seguito un VADEMECUM con alcuni pratici consigli su cosa fare e non fare.

Non visitare siti sconosciuti che promettono notizie "sensazionali" sul Covid-19. I siti ufficiali sui quali poter avere notizie sono i seguenti:

- http://www.salute.gov.it/portale/home.html
- https://www.epicentro.iss.it/coronavirus/
- http://www.protezionecivile.gov.it/home
- https://www.esteri.it/mae/it
- https://www.who.int/

Non scaricare allegati, ricevuti tramite posta elettronica o Social Network o attraverso sistemi di messaggistica, che parlino di Covid-19.

Se la tua Banca o altre istituzioni ti invitano a fare qualcosa (come accedere ad un sito, scaricare un file, inserire credenziali) per il Coronavirus, verifica che sia una richiesta lecita e motivata e non un tentativo di frode.

Più in generale, è consigliato applicare in modo ancora più vigile delle buone pratiche nell'uso dello strumento informatico e dei dati aziendali.

1. Non condividete informazioni sensibili utilizzando sistemi non governati dall'azienda.
2. Evitate l'uso di chiavette USB di cui non conoscete la provenienza.
3. Non navigate su siti Internet non sicuri o che non hanno pertinenza con il proprio lavoro.
4. Disconnettevi dalla VPN o altri sistemi di accesso remoto quando non necessari.

Quasi sicuramente il supporto IT della vostra azienda è operativo, anche se con modalità diverse, ma se non sapete come contattarlo chiedete al vostro referente.

IMQ intuity

SOCIETÀ DEL GRUPPO IMQ

Sede operativa:
Via Ceron 2, 35129 Padova
049 817 0850 | info@intuity.it

www.intuity.it