Coronavirus e telelavoro: le raccomandazioni degli ingegneri contro gli attacchi informatici

TECNOLOGIA > HITECH

Mercoledì 1 Aprile 2020

La pandemia di Coronavirus aumenta anche il rischio di attacchi informatici, perché cresce il ricorso al telelavoro e aumenta l'attività in rete di utenti relativamente inesperti di informatica, quindi più vulnerabili, con la prospettiva di danneggiare seriamente l'operatività di enti, aziende e studi professionali.

Ad evidenziare questo pericolo è il Comitato Italiano Ingegneria dell'Informazione (in sigla C3I), organismo del Consiglio Nazionale Ingegneri, che suggerisce alcune soluzioni.

LEGGI ANCHE Coronavirus, studio cinese elogia Napoli: «Il farmaco anti-artrite è efficace»

Anzitutto – come si legge in una nota - occorre dotarsi di strumenti di protezione come antivirus, aggiornandoli costantemente, **effettuare backup ogni giorno ed evitare di trasmettere informazioni sensibili tramite canali pubblici di file sharing non sicuri.**

Se proprio non si dispone di sistemi di condivisione sicuri occorre proteggere i propri dati con password più robuste (in rete sono presenti numerosi suggerimenti adatti allo scopo), usare sistemi di crittografia dei messaggi di posta elettronica e fare grande attenzione alle e-mail ingannevoli.

Per le aziende – continua la nota del Comitato – occorre dotarsi di sistemi di

TECNOLOGIA


Coronavirus, arriva l'app anti-pandemia: ecco come scaricarla


Fonte Verificata, il portale di bufale che in apparenza sembra un sito di debunking


Coronavirus, stop a tutti i giochi in tabaccheria. Resta solo il Gratta e Vinci

di Ida Di Grazia


«The governor» e il traffico: il videogame che ha per protagonista De Luca

di Giovanna Di Giorgio


Coronavirus, il Mise: falso il messaggio sul blocco delle reti per i video sui social

IL MATTINO TV


Ecco il trucco che vi lascerà letteralmente "a bocca aperta"


L'eccezionale talento di un ragazzo che fa i salti mortali...con la corda!

VIDEO PIU VISTO

analisi dei log degli accessi alle applicazioni da parte dei dipendenti, attivare sistemi di monitoraggio dei dati sensibili, **prevedere sistemi di filtraggio per evitare spam e phishing, nonché rafforzare i sistemi di backup.**

Indispensabile è anche l'aggiornamento continuo del personale dipendente sulle nuove minacce cyber, con invito al più rigoroso rispetto delle regole aziendali in tema di sicurezza informatica.
Il Comitato riassume in un'infografica (allegata) le principali regole da seguire per lavorare in modalità sicura anche da casa.

Superata la fase di emergenza, il C3I suggerisce poi tre iniziative di più ampio respiro:

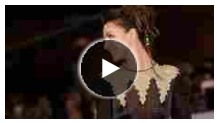
- Promuovere campagne mediatiche di sensibilizzazione su scala nazionale, per informare sulle minacce informatiche e sui rischi concreti che esse comportano per la vita della collettività.

- Istituire gruppi di lavoro ad hoc, a livello di Protezione Civile, Difesa e Interno, per l'attuazione di scenari di crisi nel caso di attacchi Cyber su scala nazionale.

- Attivare un comitato tecnico-strategico per la sicurezza informatica che includa, oltre il DIS (Dipartimento informazione sicurezza) e i competenti Ministeri, anche i rappresentanti delle Università, delle Aziende specializzate e degli Ordini professionali, nonché di agenzie europee come Enisa ed Europol.

COMMENTA

ULTIMI INSERITI PIÙ VOTATI 0 di 0 commenti presenti

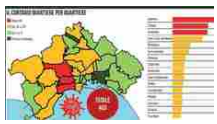


«Ambra cosa hai fatto ai denti?», la stranezza notata dagli utenti

LE PIÚ CONDIVISE

Suicidio a Salerno: 43enne si lancia dal settimo piano, è il terzo in 15 giorni

di Carmen Incisivo 10463



Coronavirus a Napoli, la mappa del contagio: il picco a Chiaia, Vomero e Arenella

di Paolo Barbuto 2923

Coronavirus e finte cremazioni, macabro business delle salme in Trentino. «Resti umani abbandonati»

14380

GUIDA ALLO SHOPPING

Gli accessori per un allenamento produttivo in casa, il miglior bilanciere per pesi