



BACK TO BASICS PER LA CYBERSECURITY

WEBINAR 15 Aprile 2020- dalle 11.30 alle 12.30



Back to Basics per la Cybersecurity

Misure e risposte concrete per mettere in sicurezza persone e processi

WEBINAR 15 aprile 2020



AGENDA

Molte aziende si pongono oggi la domanda: cosa non deve mancare nel mio Piano di Cybersecurity? quali sono le misure e i processi prioritari da prevedere, per

- *Proteggere una forza lavoro che, in questo momento, si collega in massa dalla propria abitazione*
- *Sostenere un traffico più elevato, rispondere con tempestività in caso di attacco cyber*
- *Sensibilizzare le persone, formarle per uno Smart Working in sicurezza*
- *Riposizionare la difesa tenendo conto della continua evoluzione delle minacce.*

I temi saranno affrontati nel Webinar di oggi con

- 11:30 – 11.40 **Elena Vaciago**, Associate Research Manager di **The Innovation Group**
- 11.40 – 11.50 **Corradino Corradi**, Head of ICT Security & Fraud Management di **Vodafone**
- 11.50 – 12.00 **Andrea Muzzi**, Technical Manager di **F-Secure**
- 12.00 – 12.10 **Paolo Arcagni**, Manager, System Engineering Italy & Iberia di **F5 Networks**
- 12:10 – 12:20 **Stefano Ricci**, Senior Sales Engineer di **Rubrik**
- 12:20 – 12:30 **Domande & Risposte**



channels.theinnovationgroup.it/cybersecurity



ALERT: crescita dei Rischi Cyber nei giorni dell'epidemia da Covid-19

EUROPOL



LETTERA DAL RECTOR ELIO FRANZINI

Cari colleghi,

Sto scrivendo cosa è l'essenza di CORONAVIRUS 2019-nCoV. Come altre università europee, il 28 gennaio 2020, l'Università di Milano-Bicocca ha deciso che sospendere temporaneamente tutti i viaggi previsti in Cina per studi, ricerche e conferenze fino a nuovo avviso.

Il 31 dicembre 2019, l'Organizzazione Mondiale della Sanità è stata informato di un gruppo di casi di polmonite da sarscovirus rilevata a Wuhan, nella provincia cinese di Hubei. Le autorità sanitarie cinesi hanno identificato un nuovo Coronavirus (denominato 2019-nCoV) come responsabile dell'epidemia rispettiva.

La maggior parte dei casi di sarscovirus sono solo il rischio di infettione entro il 2019-nCoV, ma anche la scarsa durata dell'epidemia, il rischio associato di dislocazione sociale nelle ore collegate o resti immobili di qualsiasi tipo, che potrebbero rendere impossibile tornare a casa.

I passi che può adottare per proteggersi dall'infettione da 2019-nCoV sono alligati in questi e-mail e tutti i dipendenti, inclusi l'impegno a tempo parziale, sono tenuti a prendere attivazione l'allegerito.

Speriamo che le situazioni miglioreranno il più presto possibile.

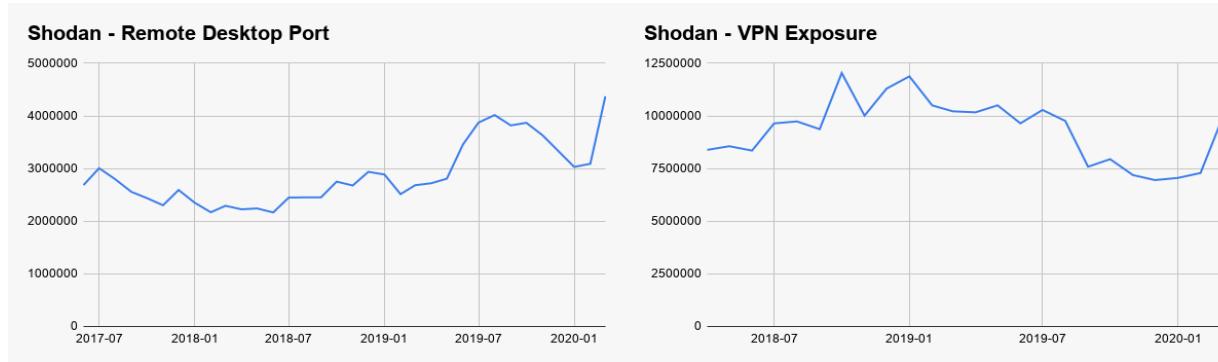




Ripensare la Resilienza con una forza di lavoro distribuita

Utilizzo di RDP in crescita del 41%, utilizzo di Enterprise VPN del 33% nelle due settimane centrali di marzo 2020

MAGGIORE
DOMANDA
DI SICUREZZA



NUOVI
RISCHI ...



VECCHI PROBLEMI ... REPORT

Smart working e didattica online? Ma il 33% delle famiglie non ha pc o tablet a casa

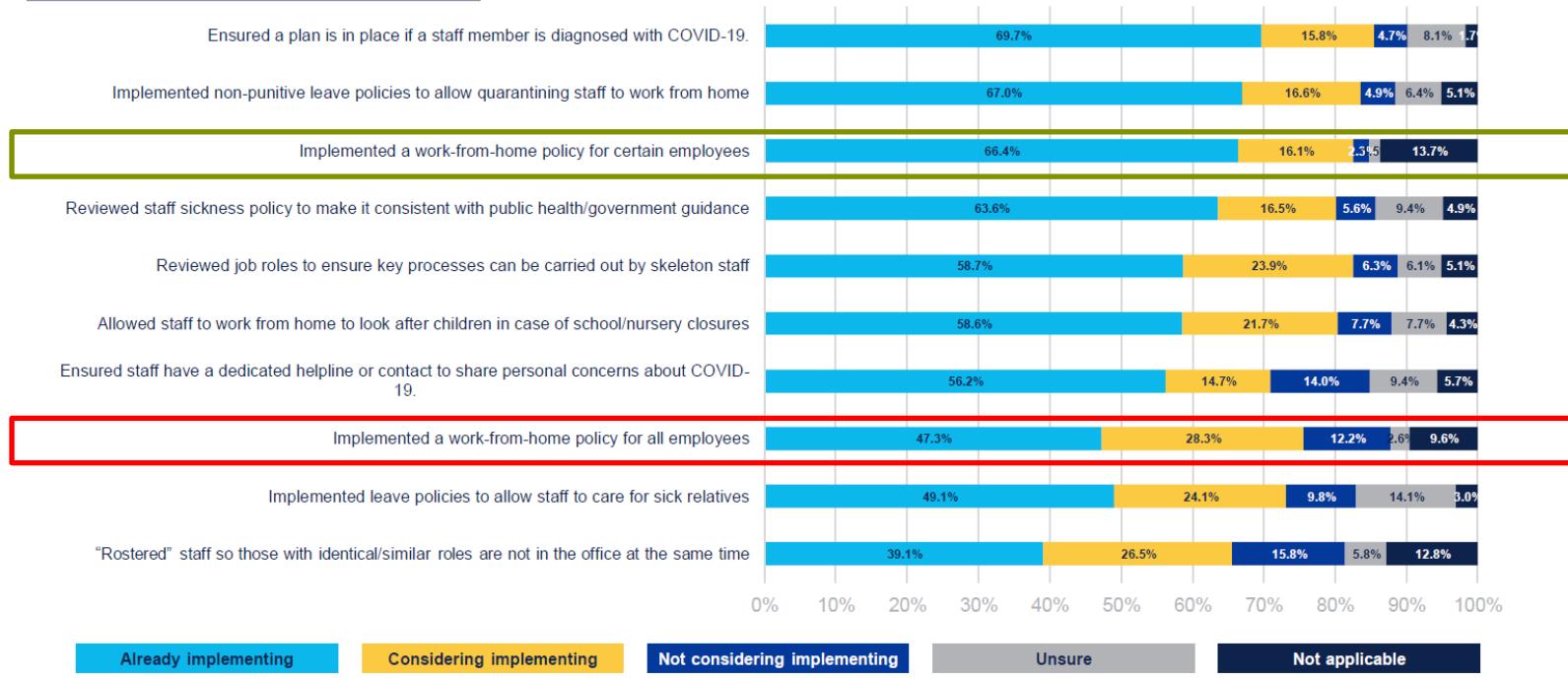
di Paolo Anastasio | 6 Aprile 2020, ore 14:45



Come affrontare l'emergenza e garantire la continuità?...

bci Leading the way
to resilience

Which of the following HR and staff measures have you taken or are considering taking in your organization?



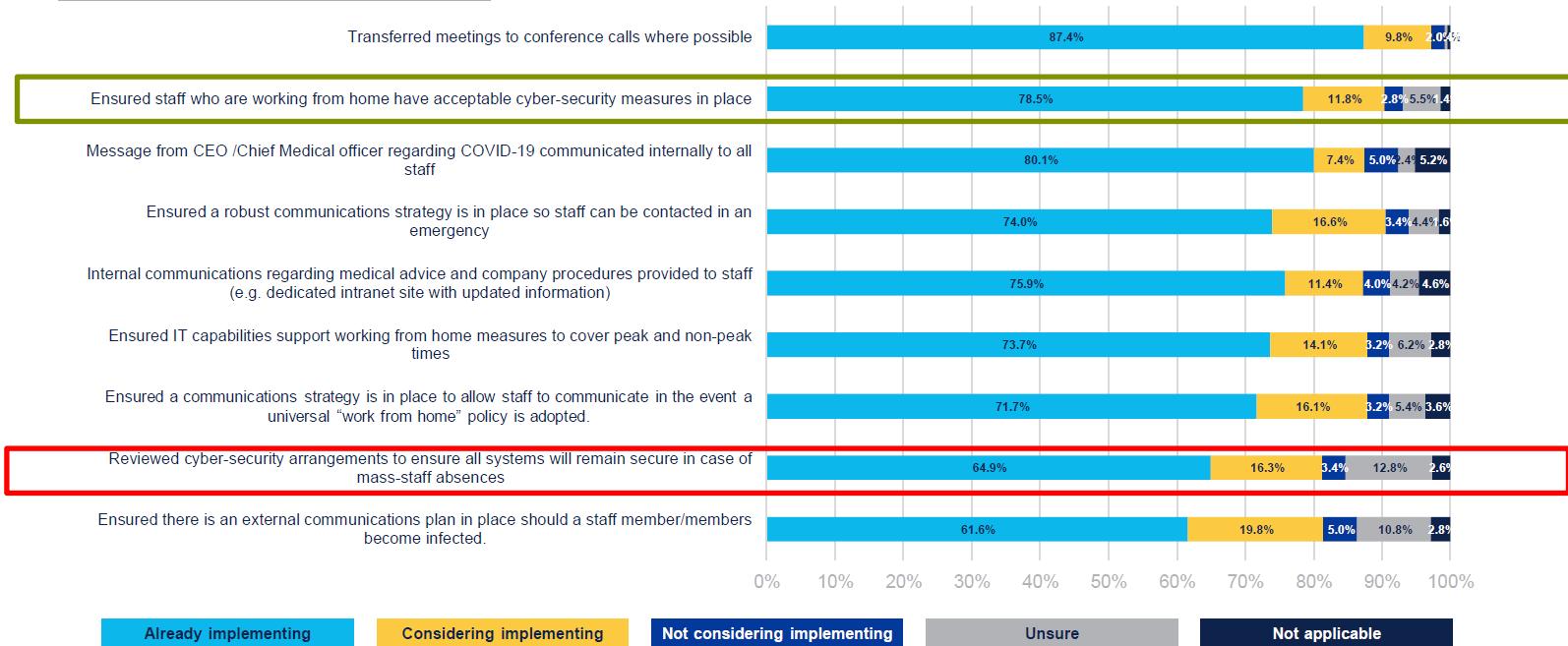
4 www.thebci.org



... e quali sono le misure da prevedere per la Cybersecurity?

bci Leading the way to resilience

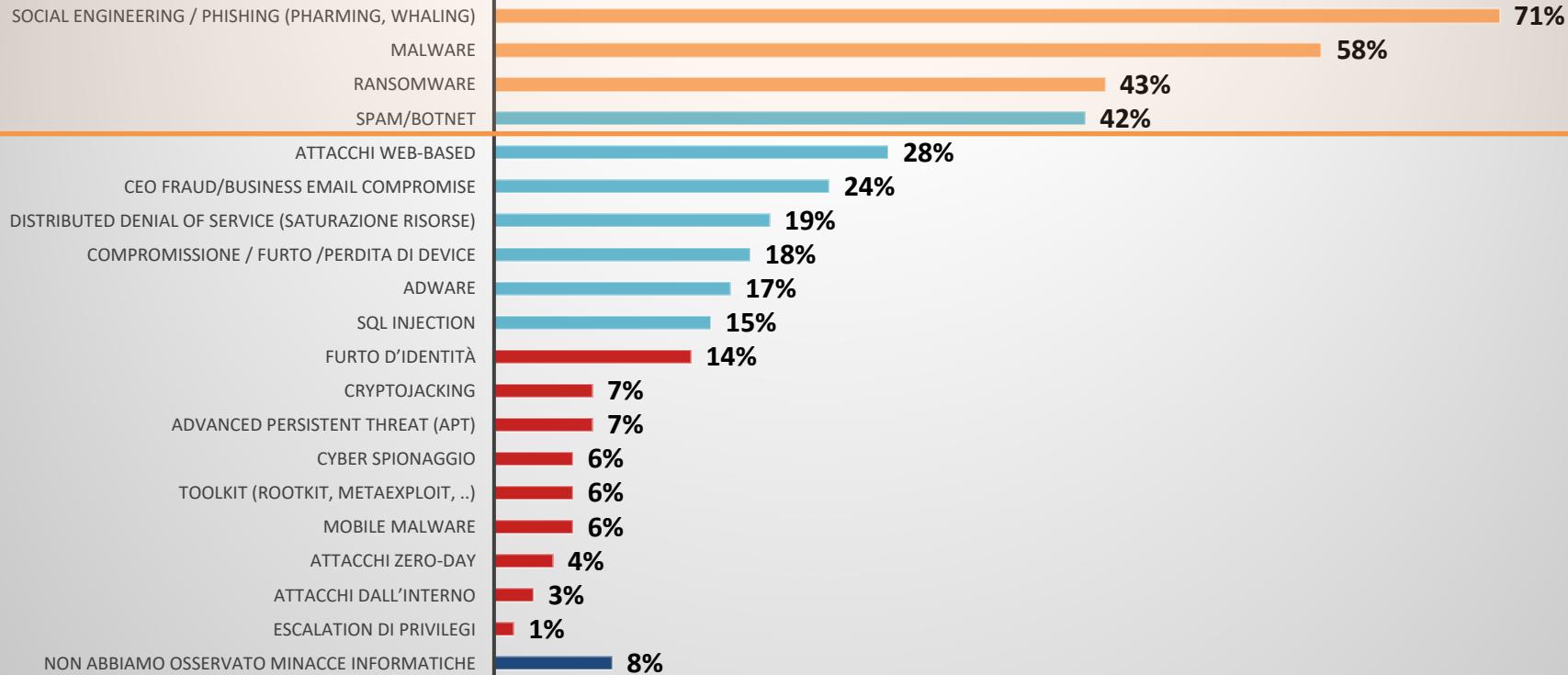
Which of the following IT, technology and communications measures have you taken or are considering taking in your organization?





Il Phishing è oggi la minaccia cyber osservata con maggiore frequenza, seguita da malware, ransomware, spam

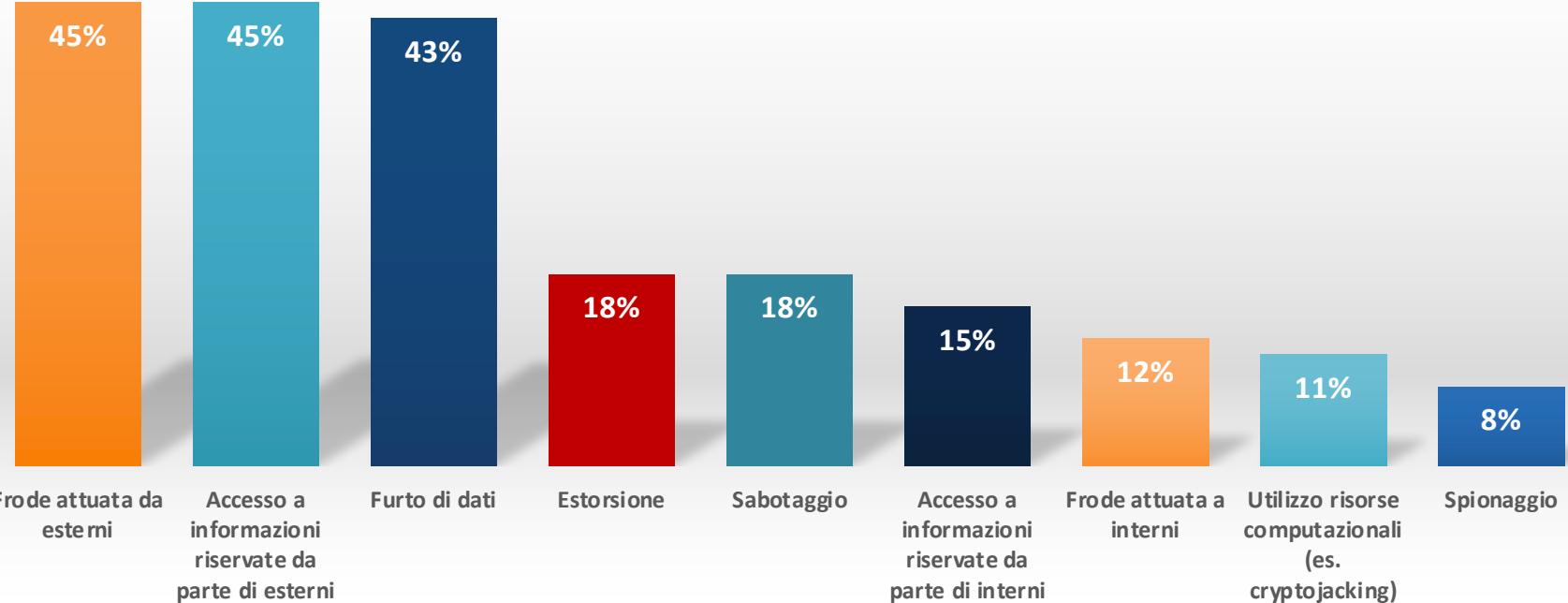
Nel corso degli ultimi 12 mesi, quali dei seguenti attacchi cyber hanno riguardato la Sua azienda?





Le motivazioni che spingono il cyber crime sono molteplici, ma prevalgono nettamente quelle a scopo economico

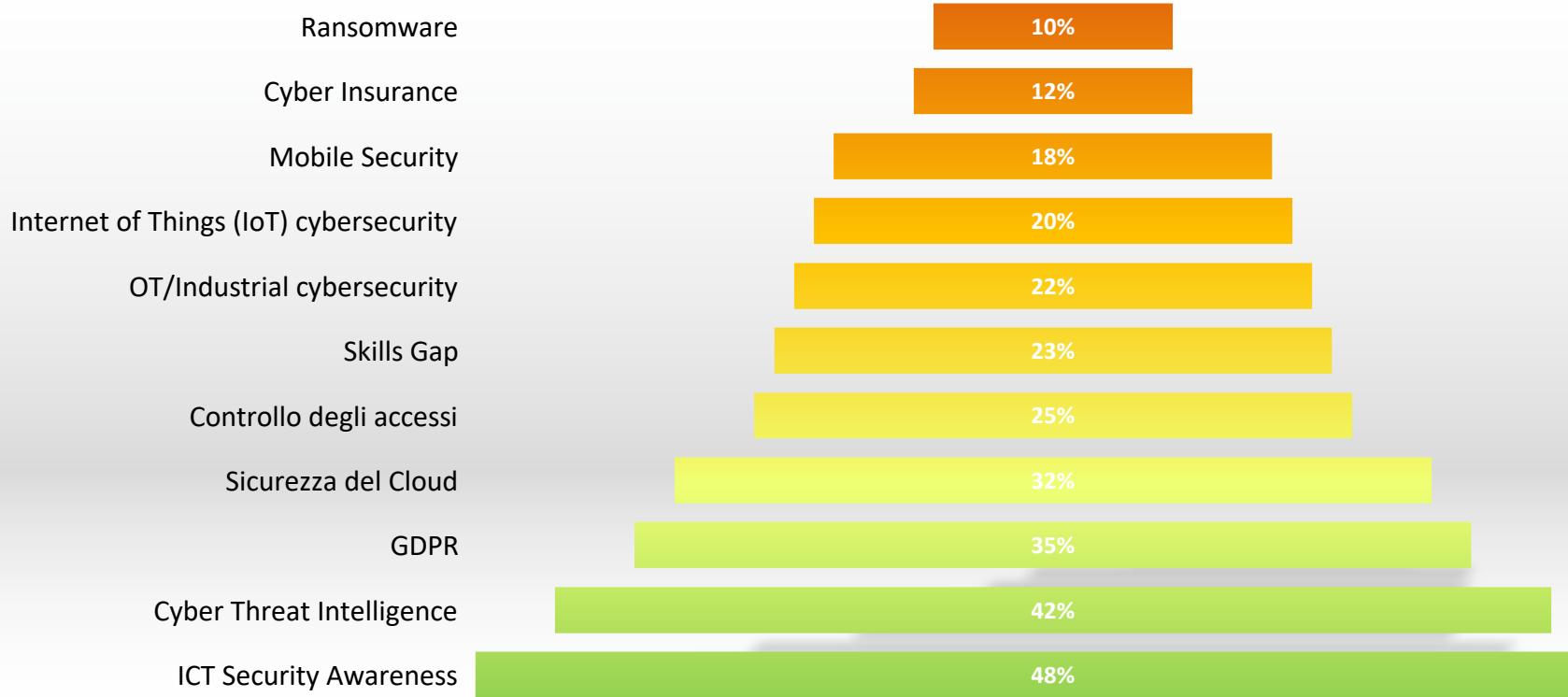
Quali erano le finalità degli attacchi osservati?





Spostamento di focus sui temi del Fattore Umano e dell'Intelligence

Quali dei seguenti Hot Topic sono secondo Lei oggi più rilevanti per un CISO/Security Manager?





Back to Basics: facciamo ordine sui «fondamentali» per la cybersecurity

SAFE TELEWORKING



National Cyber Security Centre

Stay Safe Online

Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cybersecurity policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals
Are really good at identifying what can be monetised, for example stealing and selling sensitive information from systems and information to ransom.



Foreign governments
Show a particular interest in accessing really sensitive information, or contain links to malicious websites. If an infected attachment arrives in your inbox, don't open it.



Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way to gain financial gain, or cause disruption for the sake of it.



Political activists
Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.



Terrorists
Promote their message through propaganda and disruption activities; they generally have less technical capabilities.



Malicious insiders
Sometimes staff, with the best of intentions just want to help, for example by accidentally sending something sensitive to the wrong email address.



Honest mistakes
Sometimes, staff, with the best of intentions just want to help, for example by accidentally sending something sensitive to the wrong email address.



Defend against phishing attacks

Phishing emails appear genuine but are actually fake. They might try to trick you into giving away sensitive information, or contain links to a malicious website. If an infected attachment arrives in your inbox, don't open it.



Phishers
Create fake emails containing sensitive information about you to make them appear convincing. Review your privacy settings, and think about what you post online.



Scammers
Out to make money from you. This can include urgency or authority cues that pressure you to act.



Business email compromise
Attackers will try to exploit 'normal' business communications and processes. Make sure you make it easier to spot unusual activity.



Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.



Secure your devices

The tablets, laptops or desktop computers that you use can be lost or stolen physically, but you can protect them from many common attacks.



Don't ignore software updates - they contain patches that keep your device secure. Your device will be more vulnerable if you're prompted to install any, make sure you do.



Always lock your device when you're not using it. This makes it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.



Always use official app stores (like Google Play or the Apple App Store) to download some protection from viruses. Don't download apps from unknown vendors and sources.



If in doubt, call it out
Report suspicious emails promptly - usually to your IT team or line manager - can massively reduce the potential damage of a cyber incident.



Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support from your IT team or line manager.



Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done nothing wrong, it's important to let your IT team know what's happened.



Don't be afraid to challenge the process and ask questions. Security should be at the heart of people doing their jobs, doesn't work.



Seven Imperatives to Protect Against Cyber Risks

As companies ask millions of staff to work remotely from home, they must take the following steps to safeguard their IT systems and data from cyber attack:

- 1 Assess core IT infrastructure for remote working
- 2 Secure applications and devices for the remote workforce
- 3 Embed cybersecurity into business continuity plans
- 4 Make the newly remote workforce aware of the added security risks
- 5 Establish protocols and behaviors to prepare for secure remote working
- 6 Embed cybersecurity in corporate crisis management
- 7 Update access and security measures

Source: BCG analysis.



I prossimi appuntamenti TIG: STAY TUNED!!



WEBINAR: SMARTWORKING E CYBERSECURITY

06.05.2020 – ONLINE dalle 15.00 alle 16.00



CYBERSECURITY SUMMIT ROMA 2020

02.07.2020 - Centro Congressi Roma Eventi Fontana di Trevi – Roma



GRAZIE PER LA PARTECIPAZIONE!