LA SICUREZZA IN TEMPI DI CRISI

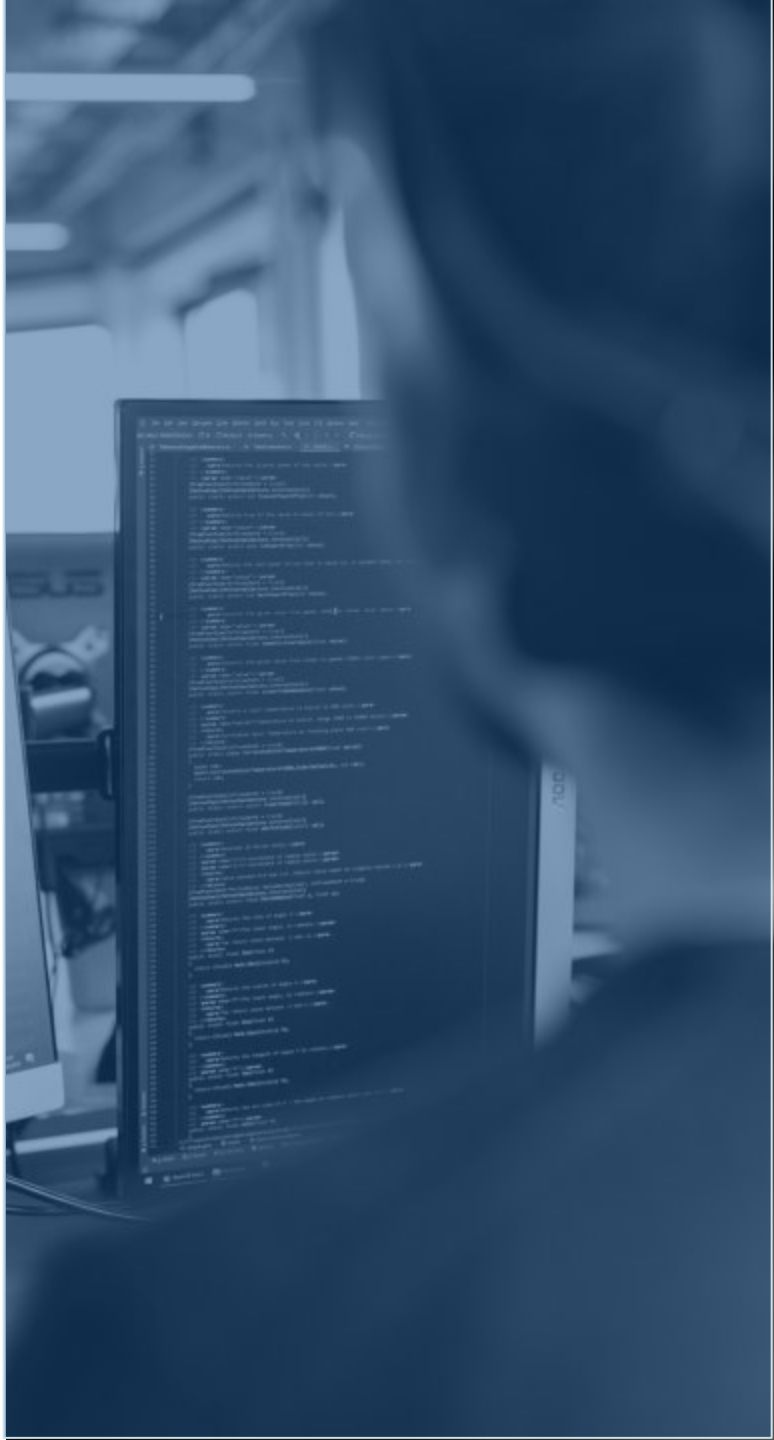
March, 2022

Powered by CYBEREADY

Perché è importante

L’attività cibernetica che circonda il conflitto Russia - Ucraina sta aumentando e, anche se non siamo direttamente coinvolti nel conflitto, siamo tutti coinvolti.

Ogni crisi mondiale ha una dimensione cibernetica e un forte aumento di e-mail di phishing malevole dimostra che questa crisi non è diversa dalle altre.



Cosa sta succedendo

1 Entrambe le parti hanno lanciato attacchi informatici l'una contro l'altra, tra i quali malware che cancella i dati e siti Web messi offline per impedirne l'uso legittimo.

2 Questi attacchi non vengono sempre contenuti e spesso infettano dispositivi e siti Web non coinvolti nel conflitto. Sono inclusi anche i dispositivi aziendali o personali.

3 I tuoi account personali sui social media sono anche a rischio di essere violati allo scopo di distribuire informazioni false o malware.

Cosa puoi fare per proteggere la tua rete domestica

Installa aggiornamenti del sistema operativo e di sicurezza. Se essi sono disponibili, dovresti vedere una notifica sul tuo computer o telefono.

Aggiungi un secondo fattore di autenticazione ai tuoi account di social media (Facebook, Linkedin, Twitter, ecc.) e ai tuoi account di posta elettronica. Se possibile, aggiungi anche un account di posta elettronica di riserva.

Fai sapere ai tuoi amici e familiari cosa sta succedendo e invitali a fare lo stesso.

Cosa puoi fare per proteggere la tua rete

Ci prendiamo cura della sicurezza della rete interna, quindi non devi fare nulla a livello tecnico.

In questi periodi potresti ricevere più attacchi di phishing. Diffida delle e-mail che richiedono il tuo intervento in questioni tecniche o finanziarie.

Continua a controllare l'indirizzo e-mail del mittente e ricorda che questo è il passo più importante per individuare un attacco di phishing.