SECURITY IN TIMES OF CRISIS

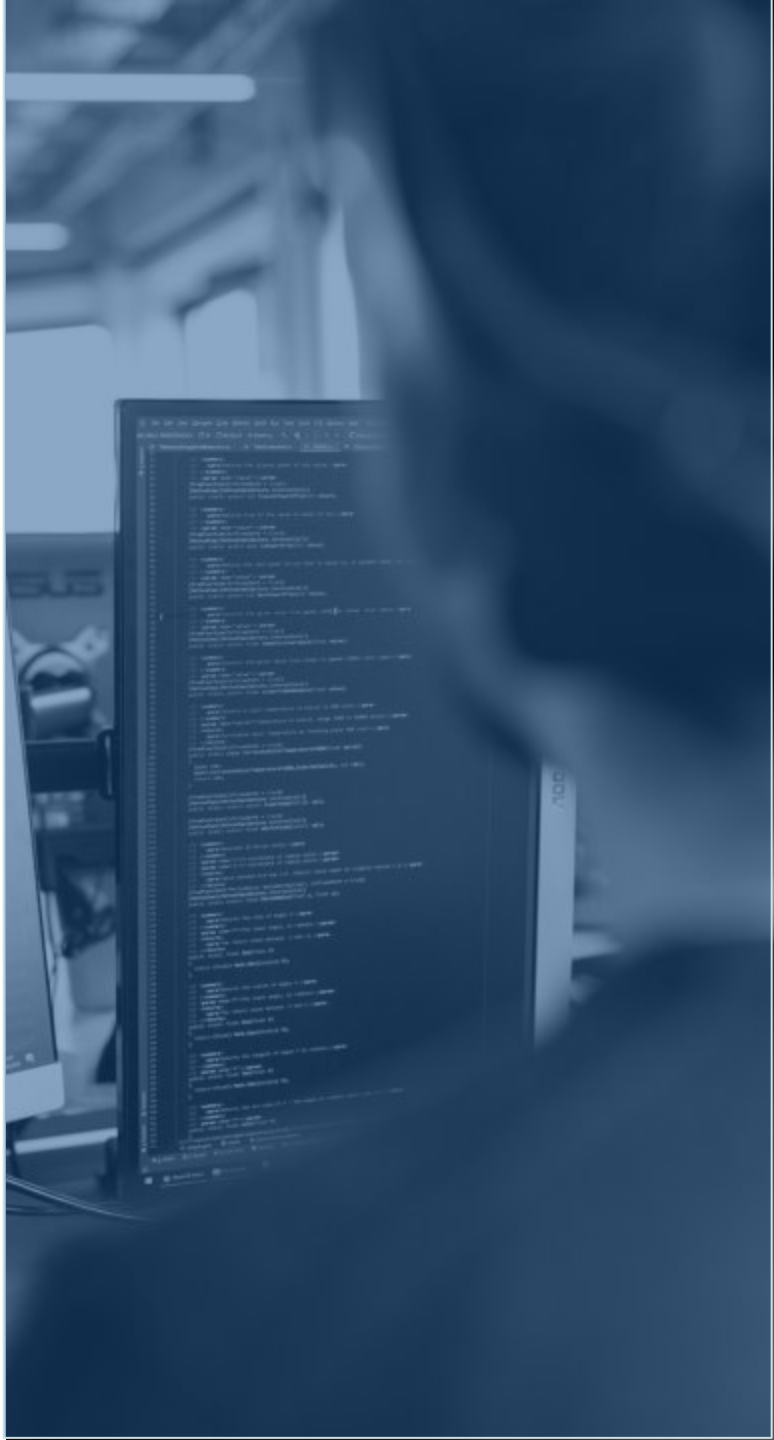
March, 2022

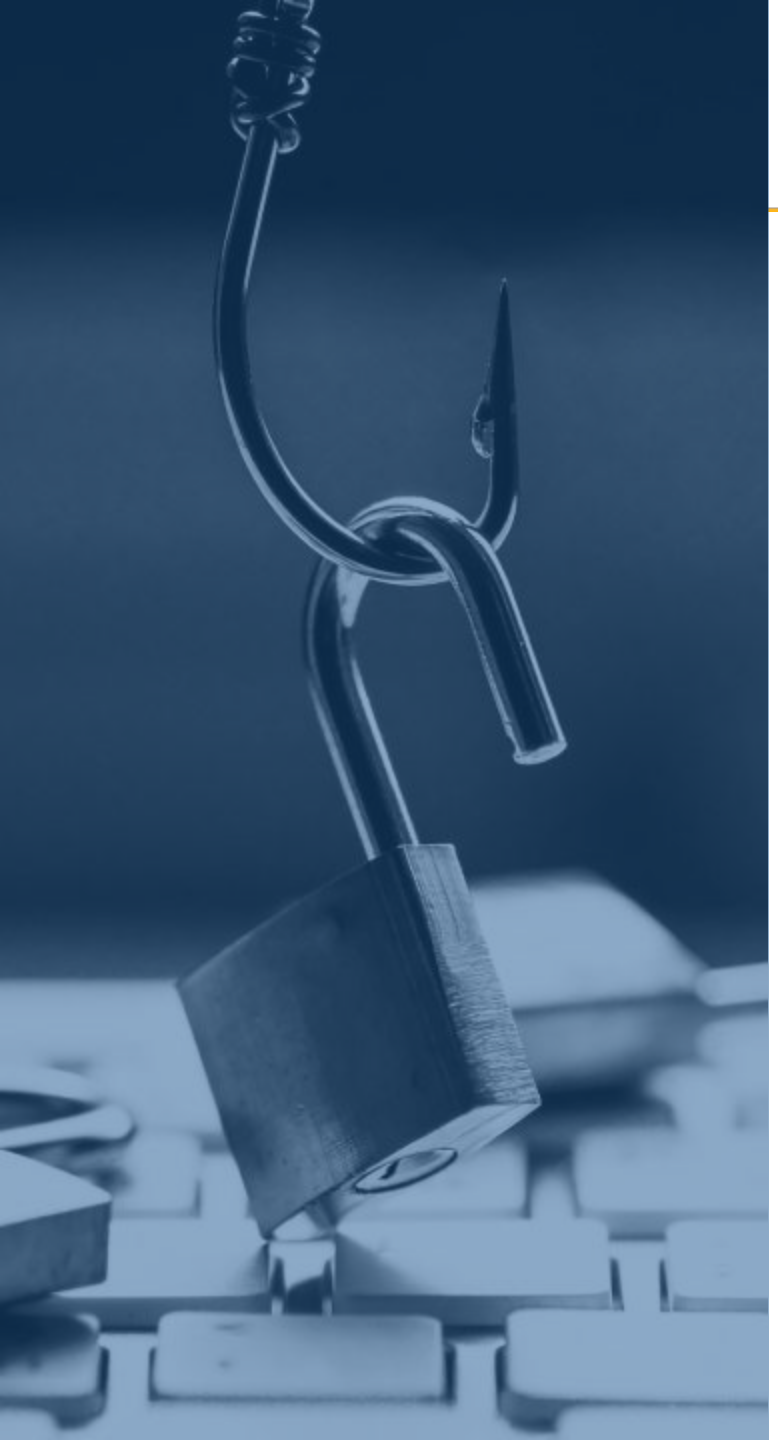
Powered by CYBEREADY

Why does it matter

Cyber activity surrounding the Russia – Ukraine conflict is surging and although we might not be directly involved in the conflict, we are all affected.

Every world crisis has a cyber dimension to it and a sharp increase in malicious phishing emails shows this crisis is no different.





What is going on

1 Both sides have launched cyber attacks on each other that include data-wiping malware and websites taken offline to prevent legitimate use.

2 These attacks are not always contained and often infect devices and websites that are not involved in the conflict. This includes your corporate or personal devices as well.

3 Your personal social media accounts are also at risk of being hacked for the purpose of distributing false information or malware.

What can you do to protect your home network

Install operating system and security updates. If these are available you should see a notification on your computer or phone.

Add a second factor for authentication to your social media accounts (Facebook, Linkedin, Twitter, etc.) and your email accounts. If possible add a backup email account as well.

Let your friends and family know what’s going on and urge them to do the same.

What can you do to protect our network

We are taking care of the internal network security, so there is nothing technical you need to do.

During these times you might get more phishing attacks. Beware of emails requesting your assistance in technical or financial matters.

Keep checking the sender’s email address – remember that this is the most crucial step in detecting a phish.