EC-Council

OHPHISH
Fortifying Front Lines

EC-Council Provides Free Phishing-Protection Solution to Help Remote Workers and Businesses Fight Phishing Attacks

Amid the outbreak of COVID-19, many businesses have been forced to move their workforce to work from home as part of a global social distancing initiative. However, not many organizations are equipped to deal with the risks of remote working. Every organization is concerned about its cybersecurity and with the rise of phishing attacks, they are especially concerned about providing security awareness training to its remote workforce.

With inadequate protection on home networks, employees are more susceptible to phishing attacks than ever before.

There have already been headlines about people all over the world being hit by Coronavirus-related phishing attacks, via emails, websites, and fake news. It is imperative that all employees remain vigilant and capable of protecting themselves from such attacks.

During this Pandemic, cybersecurity threats are high, and EC-Council is dutybound to help organizations take all necessary steps to thwart any such attempts. We are pleased to offer a FREE phishing-protection solution, OhPhish, to all organizations to enable professionals to work securely from home.

EC-Council will make further arrangements, opening up more of its core solutions, should the situation require it.

For more details: https://ohphish.eccouncil.org

Thank You,

Regards,

Jay Bavisi,

President and Chief Executive Officer,

Free Subscription to OhPhish

With the 30-day free subscription to OhPhish, organizations can now run unlimited entice-to-click simulations and assign security awareness training to all remote workers. This is just the start, a small step we take as we continue to track the developments of the COVID-19 situation.

3 Steps to Access OhPhish for 30-days

1. Visit ohphish.eccouncil.org
2.Click on 'Get Started'
3.Sign up for FREE and run a simulation for 1000 users!

Don't Get Hooked!

1.Coronavirus related fraud increases by 400% in March, with most scams related to online shopping for face masks, hand sanitizer, and other hygiene products.

2.There are over 200 reports of coronavirus-themed phishing emails tricking people into opening malicious attachments, stealing personal information.

3.The total loss has reached nearly £970,000 due to theft of details such as email addresses and passwords, banking details, and personally identifiable information.

Source: The National Fraud Intelligence Bureau (NFIB)