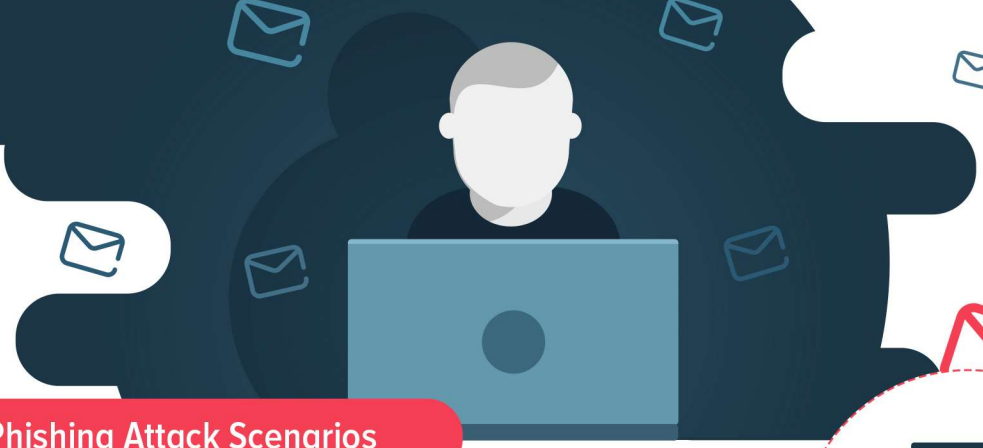
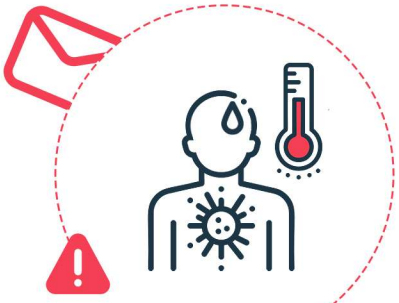
COVID-19 Phishing Scams to Avoid like the Pandemic

CyberHoot

Coronavirus Scams are everywhere, and they are ruthless and dangerous. They play upon our heartstrings and our fears by pretending to be something they are not. **Become More Aware to Become More Secure.**



Common Phishing Attack Scenarios



You May Have Been Exposed

You receive an email from a hospital email address stating:

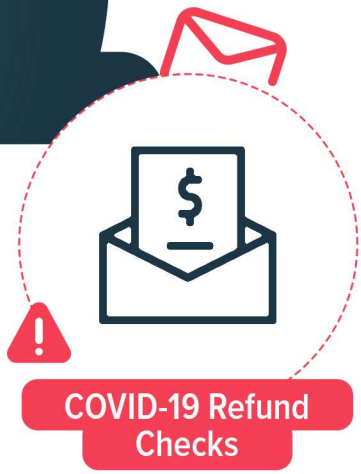
'You have been exposed to COVID-19. An infected person listed you in their contact-tracing. Complete the attached form and upload to this website to schedule your COVID test. It's your civic duty.'

Never Click links or download files from unexpected emails.

Fake COVID-19 Websites

Hackers have created hundreds of fake Pandemic Websites complete with statistics, fake treatments, and cures. Behind this bad information are malware downloads which install ransomware to encrypt your files and hold them hostage until you pay a bitcoin ransom.

Only visit reputable websites found using trusted search engines like Google, Bing, or Duck Duck Go.



COVID-19 Refund Checks

Hackers are sending Fake Refund Check emails with links and attachments that compromise your computer if you click or open them. Always ask yourself these Phishing Test questions:

Is the email:

- **Unexpected?**
- **Urging action?**
- **From an unknown sender?**
- **Generically addressed?**
- **Full of bad spelling and grammar?**
- **Linking to bad websites?**
- **Arriving with an attachment?**

If you answer yes to 2 or more questions, you are being phished. Delete the email.