neoRhino
IT SOLUTIONS

10 CYBERSECURITY BEST PRACTICES FOR WORKING FROM HOME

Cybercriminals are preying on the fear of COVID-19 through online scams intent on stealing personal and financial information. These scams are typically sent by mail or social media and claim to provide COVID-19 awareness information. It is crucial to be vigilant. Here are 10 best practices you must follow for your cybersecurity.

DON'T REVEAL SENSITIVE INFORMATION IN EMAILS

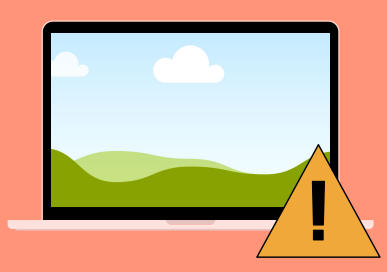
Not only is it advised to refrain from revealing sensitive information to an unverified sender, but it is also crucial to avoid responding to solicitation attempts for said credentials. If the request is unexpected, that is a potential red flag. Verify the sender before making any response.

PAY ATTENTION TO URLS

Malicious websites can look identical to legitimate sites. Always verify the URLs of any link sent to you in an email. Fake URLs typically have a different spelling and can bring you to a fake domain. If you enter in any information on a bogus website, your data could be compromised.

VERIFY THE EMAIL IS LEGIT

If you are unsure whether an email request is legitimate, verify it by contacting the company directly. If the actual name of the sender does not match the email address or the domain of the sender's email address does not match the company, these are giveaways that it could be a phish.

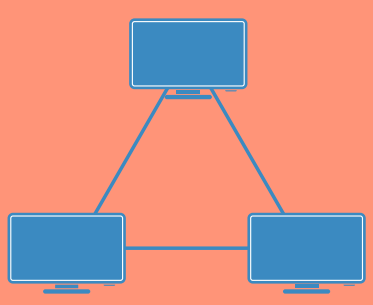


KEEP A CLEAN MACHINE

Keep all software on every internet-connected device you have operating (including PCs, smartphones and tablets) updated to the most current firmware revision to reduce risk of infection from malware.

USE SECURE NETWORKS

It is advised to use an enterprise Virtual Private Network (VPN) to access any business accounts online. All routers and access points should be updated to the latest firmware and secured with a complex password that you create. Even while using a VPN, do not connect to public Wi-Fi hotspots.



SEPARATE YOUR NETWORK

Your work and home devices should connect to separate Wi-Fi networks when possible. Keeping both devices on the same network allows a higher chance for cyber-criminals to steal information. If your router is capable, secure your company devices on one Wi-Fi band, while the other can be used for friends and family.

USE A UNIQUE PASSWORD

It cannot be stressed enough that having a unique password is essential. Using generic passwords make it easier for cyber-criminals to steal your critical data and do not use the same passwords for different logins. Use a password manager if you have difficulty keeping track of your logins.

REPORT SUSPICIOUS ACTIVITY IMMEDIATELY

To prevent any further cyberattacks on your business, report any malicious activity to your IT department immediately. This helps to increase the awareness of any potential intrusions on your network and sensitive data.

ENFORCE POLICIES AND TRAIN YOUR EMPLOYEES

As more employees are working from home due to the COVID-19 pandemic, we highly advise companies to establish security policies and guidelines for remote workers and company expectations. Provide policy training and a clear process for remote workers to reach out to your IT provider for support should any issues occur.

GO THE DISTANCE

Regardless of your location, it is imperative that all internet users stay safe and secure online by updating software on all devices (including anti-virus and firewall protection) backing up your data, enabling multi-factor authentication, and having strong, lengthy passwords for every online account.

For more information and tips visit our website at www.neorhino.com.