REMOTE WORK GUIDE DO'S AND DON'TS

AMS TECHNOLOGY

Working remotely has many benefits but also creates many cybersecurity risks. Here is a handy list of do's and don'ts to help you protect your company and sensitive information!

DO
Read & acknowledge your company's Remote Work and Bring Your Own Device (BYOD) policies and procedure

DON'T
Ignore the guidelines in your company's policies. Make the required changes if any

DO
Avoid using your personal device for work and restrict the use of company-issued devices for personal use

DON'T
Let family members or friends use your company-owned devices

DO
Protect the data you are accessing by using a Virtual Private Network (VPN) to log into the company network

DON'T
Use public Wi-Fi to access the company network without using a Virtual Private Network (VPN)

DO
Use strong unique passwords on all your devices and accounts to prevent unauthorized access

DON'T
Use your default Wi-Fi router password

DO
Ensure all personal devices are secure with anti-virus and anti-malware software

DON'T
Forget to update your router's firmware and ensure the software on all devices within your home network is kept up to date

DO
Be extremely cautious of email phishing scams

DON'T
Send electronic payments without following your company's policy for verifying payment requests

REMOTE WORK GUIDE TIPS FOR SUCCESS

ESTABLISH EXPECTATIONS

Know what your company is expecting of you and let your supervisor know if you have concerns or questions

CREATE A PRODUCTIVE ENVIRONMENT

Have a dedicated space so you can separate your work from home

GET IN A PROFESSIONAL MINDSET

Do what you normally do before work. Get a shower, get dressed, etc.

TAKE BREAKS

Set timers to take breaks, take a lunch, go for a walk, etc. It's okay to temporarily turn off your work

STICK TO A PLAN

Have start and finish times each day

FOCUS

There are plenty of distractions when working from home. Find what helps you stay in the groove

CONNECT WITH YOUR CO-WORKERS

Working remotely can make you feel isolated. Check-in with your co-workers throughout the day for some conversation

AMS
TECHNOLOGY

REMOTE WORK GUIDE PHISHING TIPS

Phishing emails are a common attack vector used by cybercriminals. Working from home creates new opportunities for these scammers to try to trick you!

BE WARY OF EMAILS THAT:

Are sent from a suspicious sender's address

Ask you to confirm personal information

Ask you for financial information

Include grammatical and spelling errors

Use threatening language or instill panic

Include a suspicious attachment

Request that you click a link

Ask you to change a password or confirm credentials

LOOKING FOR MORE TIPS OR GUIDANCE ON HOW TO SAFELY WORK FROM HOME? CONTACT US!

brad@amstechnology.net

AMS TECHNOLOGY

Phone: 253-848-5968
www.amstechnology.net