ABACODE

TOP 10 SOCIAL DISTANCING CYBERSECURITY TIPS | BUSINESS

10 COMMUNICATION

Communication isn't just allowed, it's a must for remote work! COVID-19 doesn't spread over the phone. Make sure your employees know who to call if they see something strange on their machine, get a strange request from inside our out of your organization. Don't call any number provided by the suspicious source if you can help it.

9 BACKUPS

Ensure you have backups of everything. Storing data in a secure cloud or data center is ideal in case local machines are compromised and locked out of malware.

8 MULTI-FACTOR AUTHENTICATION

Nobody is perfect, and if passwords or systems should be compromised try to make sure there's multi-factor authentication on everything to slow down or stop an attack.

7 TRAINING

Mistakes happen. Be sure to train employees on common attacks and compromises and how to protect themselves against them. Phishing training is available from many sources.

6 SIEMs

Managed SIEMs (Security Information and Event Management)are helpful tools that can be used to help identify if one of your identified assets is compromised.

BONUS TIP!

Stop having default passwords on devices like routers and printers.

1 DOCUMENTATION

Make sure your documentation is up to date! BCDR procedures often don't get updated until they're needed and the flaws are found. Before it happens to you make sure your internal policies plan for the pitfalls of working remote like remote user compromise. Failing to plan is planning to fail.

2 BE AWARE

Be aware of what assets are accessing company data. Anything that touches email, databases, etc should have management software of some kind.

3 SOFTWARE MANAGEMENT

As well as knowing all hardware on your network, software management should also be well-maintained. Make sure all hosts are fully patched as well as the programs like web browsers, file readers, and company chat programs like Slack and Microsoft Teams installed on them.

4 ADMINISTRATOR ACCESS

Avoid giving employees local administrator access if possible. The temptation is great with social distancing but a secure remote management system accessible only within a VPN is better than risking compromise.

5 VPNs

Speaking of: VPNs. Keep everything on a secured, monitored network you control. Make sure all your employees can and are connecting to the VPN.