GUARDSIGHT

https://www.guardsight.com

Cybersecurity Tips For IT Administrators When Working From Home

YOUR AWARENESS IS THE BEST DEFENSE

Cyber attackers are conducting passive reconnaissance on companies to locate their IT Administrators as high-value targets for manipulation and subsequent access into corporate networks. Be aware of this and carefully review all communications before clicking or responding. Common sense is your friend!

PRO TIPS

- ➢ Secure your home networking devices
- ➢ Keep company assets separate from personal assets
- ➢ Patch personal assets and network devices
- ➢ Use multifactor authentication
- ➢ Hide company assets from home and guest devices
- ➢ Prohibit others from using company devices
- ➢ Use antivirus or endpoint detection software
- ➢ Use common sense

For additional advice or to learn more contact us: info@guardsight.com

1	SEPARATE/SEGMENT ASSETS	1. Use personal assets for personal purposes and company assets for work purposes and avoid the temptation mix out of convenience. 2. Hide company assets from being discovered by personal home assets. 3. Avoid sending company emails from personal email services and vice versa. 4. Prohibit others from using company devices.
2	USE MULTIFACTOR	1. Use multifactor authentication whenever possible.
3	COORDINATE WITH SECOPS	1. Inform the Cyber SECOPS team when you plan to conduct administrative activities such as user adds, moves, and changes. 2. Provide the Cyber SECOPS team with some attributable friendly information such as likely IPV4/IPV6 GEO, typical hours of non-operation, most used browser characteristics, and types of mobile devices.
4	AVOID PHISHING ATTACKS	1. Email or text messages from unknown sources that convey a sense of urgency, or crisis laden deadlines, could be a phish. 2. Be aware that threat actors may use social engineering techniques, including getting you to believe they are a fellow employee who needs IT assistance. 3. Personal email may be a target and used as a gateway into your corporate environment - SEE #1 SEPARATE/SEGMENT ASSETS.
5	PROTECT KEYS	1. Protect private keys used for orchestration, DevOps, or maintenance. 2. Rotate private keys when possible and shred unused keys. 3. Audit accounts that make use of keys to perform administrative functions.