Home Office Security Tips for Business

by Kevin D. Murray, CPP, CISM, CFE

Home office security vulnerabilities…

Home offices lack the considerable security protections afforded by the corporate environment. No access control. No IT security. No secure wastepaper disposal. No protections against electronic surveillance. Nada. Zippo. Nothing, except perhaps the family dog.

Your home office employees are vulnerable. This fact has not escaped the attention of the hackers, spies, and opportunists. They want your intellectual property. The want to know your secret strategies. They want your information, and all are now much easier to get.

Give them some help…

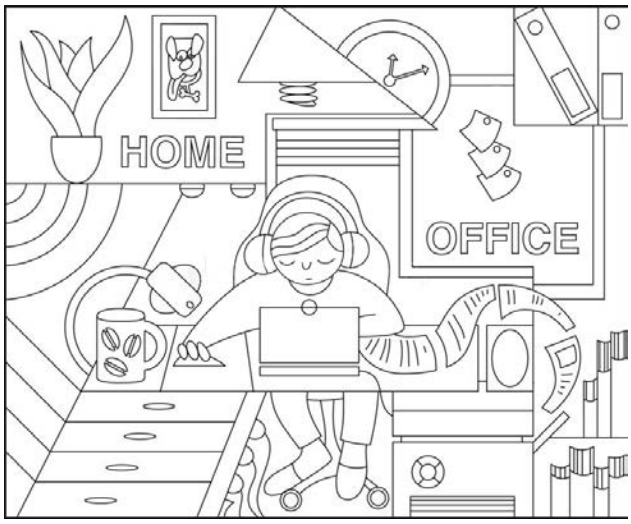
- First: If they don't have a crosscut shredder, give them one. This is important.

- Second: Create a **Home Office Security Policy**. Establish a minimum acceptable standard for information protection. Include everything from work space access control, to document protection, to communications security.

Home office security basics…

1. Create a **Self-Service Portal**
"What's that?", I hear you say.

"A self-service portal is a website, consisting of self-service and self-help functions, that enables and empowers the employee to request services, find information, and register and resolve issues. A self-service portal can be thought of as the "electronic front door" to the



IT organizations' "store", from which the consumer can obtain products and services.

From simple administrative functions such as resetting passwords and reporting incidents, to more complex actions, such as downloading software and taking corrective actions in response to issues, a well-designed self-service portal is invaluable to a consumer community that is "always on, always connected."[1]

Include a security 'how to' section. Don't assume everyone knows about VPNs, or how to connect to their wireless printer securely.

2. Communications Equipment. Inventory the systems, and the software they are using. Check that the security settings are on, encryption is being used, software security is up to date, and firmware is current. This can be handled during a routine Technical Surveillance Countermeasures (TSCM) visit.

[1] https://www.sysaid.com/cookingit/what-is-a-self-service-portal

Home Office Security Tips for Business

by Kevin D. Murray, CPP, CISM, CFE

3. Communications. Digital communications with the company needs to be routed through a Virtual Private Network (VPN).[2]

Consider providing a company VoIP telephone set (or softphone[3]) so employees can keep the conveniences provided by their office phones. This should also be routed through the VPN.

4. Encrypt. Encrypt everything you can encrypt. This includes Wi-Fi, data storage devices, teleconferences, and phone calls requiring confidentiality.

5. Email Attacks. Rule #1: Don't click on anything without being **sure** it is legitimate. Crooks view employees working from home as soft targets. The fake emails are now more sophisticated and aggressive than ever. Scams, malware, impersonations, ransomware, and spyware are flooding email boxes.

Make sure employee devices are fine tuned to dump spam, and computers have anti-malware safeguards[4] installed. Consider installing screen savers with security reminders.[5]

6. Web Filtering. Employees' computers should employ web filtering which updates automatically. This will reduce the chances of being diverted to a malicious website, and keep them on work appropriate sites.

7. Security Inspections. The work is the same. The venue is different. The risks are higher. The security inspections routinely performed at the corporate offices now need to be done at a residence.

Most of the previous recommendations can be handled during a specially crafted TSCM visit.[6] Unless there is a specific issue, once every six months should be sufficient.

***

If you have any questions, or would like to schedule home office TSCM / information security audits, just let me know.

Kevin D. Murray CPP, CISM, CFE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[7] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

You're Smart. Hire Smart.

---

[2] https://en.wikipedia.org/wiki/Virtual_private_network

[3] https://en.wikipedia.org/wiki/Softphone

[4] https://www.techradar.com/best/best-malware-removal

[5] https://counterespionage.com/media/information-security-awareness-screensavers/

[6] https://counterespionage.com/advanced-tscm-explained/residential-tscm-inspections/

[7] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/