The 10 Tenets of OpSec

Operations Security, or OpSec, is the mindset of using secure practices. Practicing OpSec helps keep us safe from ne'er-do-wells.

1 Secure your space

Don't leave sensitive documents out when away from your workspace. Lock them away when you leave your desk, and if you can't, get them out of sight.

2 Stay aware of your surroundings

Pay attention to tailgaters, shoulder surfers, and strangers. If you see a stranger in the office without a badge or ID, direct them to the security desk.

3 "For your eyes only"

If your organization classifies data as sensitive, private, or confidential, label documents and files so people can understand how they should be handled. If you discover sensitive information that's not properly protected, report it immediately.

4 Use stronger passwords

Longer is stronger. Instead of easy-to-crack passwords like Password1!, use a passphrase, like 1 Red Elephant Balloon Maker?, or a sentence you can easily remember. Or use a password manager to create and store secure passwords.

5 Don't mix business and leisure

When you use work email for Internet play, you give the bad guys more opportunities to get in. Use work email for work, and your own email for personal matters.

6 Secure your personal devices

If you use your own cellphone or laptop for work ("bring your own device" or BYOD), use anti-virus software and keep your computer and applications updated. If you have a work laptop or device, use it only for work and don't expose company assets to unnecessary risk.

7 Don't get "attached"

Word documents and PDFs can hide exploits sent by a hacker. Opening the file or enabling macros can give an attacker control over your computer. If you get an unexpected or strange email attachment from someone you know, call to check whether it's legit.

8 Use it and lose it

If you find a stray USB drive or removable hard drive, don't plug it in. It's old hacker trick to litter the area around an office with infected USB devices. Don't plug in a hacker's weaponized USB, send it to IT!

9 Beware of Wi-Fi eavesdropping

Bad actors can easily impersonate known Wi-Fi connections using a cheap device that can kick you off a router and fool your device into happily accepting a faster connection. Don't ignore browser warnings. Use a secure virtual private network (VPN) or tether to your own phone or hotspot.

If you have to use an untrusted connection, avoid sensitive activities like online banking or logging into work webmail.

10 Travel smart

On a plane, train, or public transit, you're not protected like at the office. Privacy screens help keep your work private. Lock your computer when you're not using it, and lock up laptops and sensitive documents safely when you're done for the day. Take sensitive documents back home if you can't dispose of them securely.

Lodestone SECURITY

Source: Lodestone Security, www.lodestonesecurity.com, info@lodestonesecurity.com

beazley