IT Security DOs and DON'Ts

SOPHOS
Cybersecurity made simple.

1

Don’t be tricked into giving away confidential information

Don’t respond to emails or phone calls requesting confidential company information— including employee information, financial results or company secrets. It’s easy for an unauthorized person to call us and pretend to be an employee or one of our business partners.

Stay on guard to avoid falling for this scam, and report any suspicious activity to IT. And protect your personal information just as closely.

2 Don’t use an unprotected computer

When you access sensitive information from a non-secure computer, like one in an Internet café or a shared machine at home, you put the information you’re viewing at risk.

Make sure your computer is running the latest approved security patches, antivirus and firewall. And you should work in user mode, not administrator mode, whenever possible.

3 Don’t leave sensitive info lying around the office

Don’t leave printouts containing private information on your desk. Lock them in a drawer or shred them. It’s very easy for a visitor to glance down at your desk and see sensitive documents.

Keep your desk tidy and documents locked away. It makes the office look more organized, and reduces the risk of information leaks.

4 Lock your computer and mobile phone when not in use

Always lock your computer and mobile phone when you’re not using them. You work on important things, and we want to make sure they stay safe and secure.

Locking your phone and computer keeps your data and contacts safe from prying eyes.

5 Stay alert and report suspicious activity

Always report any suspicious activity to the IT team. Part of our job is to stop cyber attacks and to make sure our data isn't lost or stolen.

All of our jobs depend on keeping our information safe. In case something goes wrong, the faster we know about it, the faster we can deal with it.

6

Password-protect sensitive files and devices

Always password-protect sensitive files on your computer, USB, smartphone, etc.

Losing items like phones, USB flash drives and laptops can happen to anyone. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data.

7

Always use hard-to guess passwords

Don’t use obvious passwords, like “password,” “cat,” or obvious character sequences on the qwerty keyboard, like “asdfg” and “12345.” It’s better to use complex passwords.* Include different letter cases, numbers, and even punctuation.

Try to use different passwords for different websites and computers. So if one gets hacked, your other accounts aren’t compromised.

*$e7enal1ig@t0r5inmyb^th (seven alligators in my bath)

8 Be cautious of suspicious emails and links

Don’t let curiosity get the best of you.

Always delete suspicious emails and links. Even opening or viewing these emails and links can compromise your computer and create unwanted problems without your knowledge.

Remember, if something looks too good to be true, it probably is.

9 Don’t plug in personal devices without the OK from IT

Don’t plug in personal devices like USB flash drives, MP3 players and smartphones without permission from IT.

These devices can be compromised with code waiting to launch as soon as you plug them into a computer.

Talk to IT about your devices and let us make the call.

10 Don't install unauthorized programs on your work computer

Malicious applications often pose as legitimate programs, like games, tools or even antivirus software.

They aim to fool you into infecting your computer or network.

If you like an application and think it will be useful, contact IT to look into it for you before installing.

Cybersecurity made simple with a little IT security know-how.

SOPHOS