



Top 10 Cyber Security Tips

Enterprise Edition

Enterprise computing environments contain a vast amount of resources which make them a huge target for cyber criminals. Ensure that your enterprise is protected by following these simple steps.

1	Use strong passwords and don't share them – Passwords should meet complexity and history requirements. They should not contain information such as your first or last name and they should be changed regularly.
2	Don't click on suspicious links and attachments – Phishing is frequently used by cyber criminals to capture personal and/or financial information from the unsuspecting victim. Be wary of unsolicited emails and remember that they can be spoofed to appear as a legitimate source.
3	Ensure staff have the access to do their job but not do harm – The principle of least privilege states that the subject must be able to access only the information and resources that are necessary for its legitimate purpose.
4	Identify critical systems and data and protect them appropriately – Ensure that your most sensitive and critical infrastructure, applications, and data are adequately protected. Cyber criminals seek to exploit vulnerabilities in these areas.
5	Encrypt sensitive data in transit and at rest – Encryption makes information unreadable unless decrypted with the correct key or password.
6	Patch your systems regularly to ensure operating systems and applications are up to date – Keep your operating system and software programs up-to-date with the latest security patches. Ensure that updates are applied regularly to the operating system and ALL the software programs installed on the computer.
7	Use technical controls on servers, desktops, mobile devices, and wireless (eg. anti-virus, anti-malware, logging) – There are four essential types of security software that should be active on your computer: anti-virus software, firewall, specialized file deletion software, and encryption software.
8	Use a layered defense on your network (eg. firewall, intrusion prevention, web content filtering, email content filtering) – Defense in Depth is an information assurance concept in which multiple security controls are placed throughout an IT system to provide redundancy.
9	Test the effectiveness of your defenses (eg. vulnerability scans, penetration tests, phishing campaigns) – It is vital to regularly evaluate the security controls implemented in your enterprise. This information will assist your organization successfully navigate the security threat landscape.
10	Educate your employees about risks and security hygiene (eg. security awareness program, annual security course) – With increased understanding of security awareness, users will be better able to identify a potential risk or threat and avoid becoming a victim.

