



cyber security basics

By now, we all recognize that the internet is a great resource and convenience for businesses. At the same time, it's created opportunities for a new breed of criminal – the cyber thief. Education and proactive measures are the best defense against an attack on your company's online security. Here are a few basic do's and don'ts for ensuring web security:

Web Safety and Security – Do's

- Change passwords often and use complex passwords
- Install antivirus software and keep definitions updated
- Install personal firewalls and keep rules updated (in white list mode)
- Install enterprise firewalls and keep rules updated (in white list mode)
- Install web filtering software and keep lists updated (in white list mode)
- Keep security patches current
- Monitor and archive all security logs (Antivirus, firewalls, filtering, patching...)
- Backup critical data often and save original installation media
- Implement dual control for sensitive accounts and critical systems
- Restrict access to sensitive data
- Constantly check for unusual activity on sensitive accounts and critical systems
- Maintain separate user IDs when working with sensitive accounts and critical systems
- Maintain separate workstations when working with sensitive accounts and critical systems

Web Safety and Security – Don'ts

- Do not open emails from unknown sources
- Do not install software from unknown sources or unknown websites
- Do not write down passwords in common areas
- Do not click on unknown internet links
- Do not give out information about security measures

Resources

Business Oriented

staysafeonline.org/index.html

sba.gov/beawareandprepare/cyber.html

Technical

us-cert.gov/index.html

isc.sans.org

