Protect Your Workplace

Cyber Security Guidance

Employees

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your user names, passwords, or other computer/website access codes to anyone.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Management & IT Department

- Implement Defense-in-Depth: a layered defense strategy that includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

Homeland Security

Report a computer or network vulnerability to the U.S. Computer Emergency Readiness Team

Incident Hotline: 1-888-282-0870

or

www.US-CERT.gov

For more cyber tips, best practices, "how-to" guidance, to sign up for technical and non-technical cyber alerts, and to download this poster, visit www.US-CERT.gov

DHS/PD/OIP/RMD/Feb06/v1.0