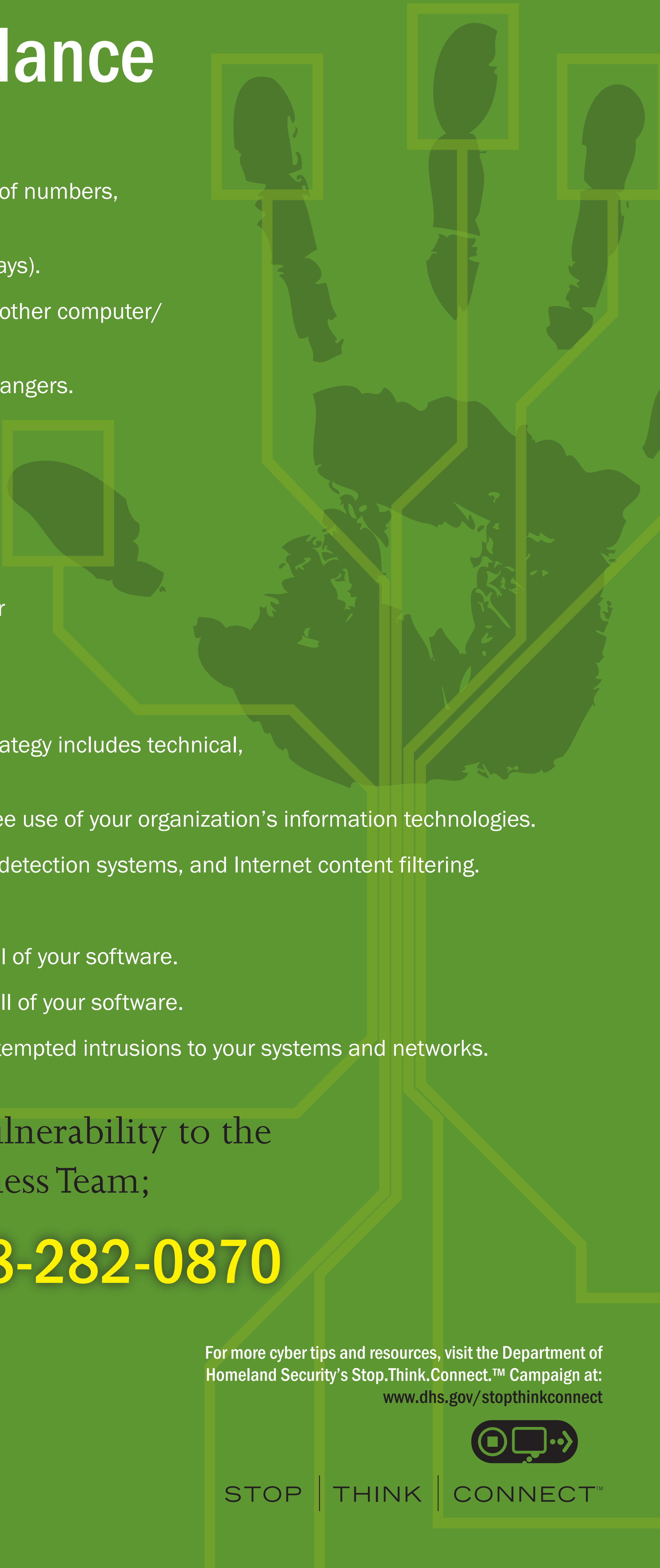
Protect Your Workplace

Cybersecurity 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 usernames, passwords, or other computer/ website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network without permission from your IT department.
- Make electronic and physical back-ups or copies of all your important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Leadership & IT Professionals

- Implement Defense-in-Depth: a layered defense strategy 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 system's 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, analyze, and report successful and attempted intrusions to your systems and networks.

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

Incident Hotline: 1-888-282-0870

www.US-CERT.gov

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at: www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™