

CYBER SECURITY TIPS

Employees:

- Use a complex alphanumeric password with a combination of numbers, symbols, and letters (uppercase and lowercase)
- Change your passwords regularly
- Do NOT open emails or attachments from unfamiliar sources, even if they look official
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department
- 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
- 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

REPORTING

Report all suspicious cyber incidents to your facility security officer:

System Failure or Disruption

Has your system or website's availability been disrupted? Has service been denied to your system's users?



Suspicious Questioning

Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware?

Unauthorized Access

Are you aware of anyone attempting (whether successfully or not) to gain unauthorized access to your system or its data?

Unauthorized Changes

Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

Suspicious Emails

Are you aware of anyone in your organization receiving suspicious emails that include unsolicited attachments and/or requests for sensitive information?

Unauthorized Use

Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?



Cyber SECURITY

Report suspicious activity to your local security contact.
Your DSS point of contact is:



This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

Industrial Security Letter 2010-02 reminds cleared contractors that all incidents must be reported to the Federal Bureau of Investigation and DSS, as specified in NISPOM paragraph 1-301.

THE WHAT



The Threats

- Insiders
- Terrorists
- Hackers
- Organized Crime
- Cyber Criminals
- Foreign Intelligence Entities

What are the actors targeting?

- Sensitive company documents
- Export-controlled technology
- Information on Department of Defense-funded contracts
- Sensitive technological specification documents
- Usernames and passwords for login
- Personal Identifying Information (social security number, date of birth, address)
- Contact rosters and phone directories

THE WAYS



How do the actors compromise our systems?

- Emails with malicious links or attachments
- Un-patched or outdated software vulnerabilities
- Removable media (USB drives)
- Use of weak or default passwords
- Website vulnerabilities
- Increased attacks against PKI credentials (i.e., stolen logon credentials)
- Spoofing emails that imitate valid domains (i.e., .mil or .gov addresses)

THE PROCESS

Anatomy of a computer intrusion:

1 Reconnaissance: Attackers research and identify individuals whom they will target through open source means.

2 Intrusion into the network: The actors send spear-phishing emails to targeted users within the company with spoofed emails that include malicious links or attached malicious documents.

3 Obtain user credentials: Attackers get most of their access using valid user credentials. The most common type: domain-administrator credentials.

4 Establish a back door: With domain administrative credentials, the actors will move laterally within the victim's network, installing back doors for future and continued exploitation.

5 Install multiple utilities: Utility programs are installed on the victim's network to conduct system administration, steal passwords, get email, and list running processes.

6 Data exfiltration: The actors obtain emails, attachments, and files from the victim's servers and then encrypt and exfiltrate the data via the actor's command & control infrastructure.

7 Maintaining persistence: If the actors suspect they are being detected or remediated, they will use other methods to ensure they don't lose their presence in the victim's network, including updating their malware.