Cyber Hygiene

Golden Rules Of Netiquette

Introduction

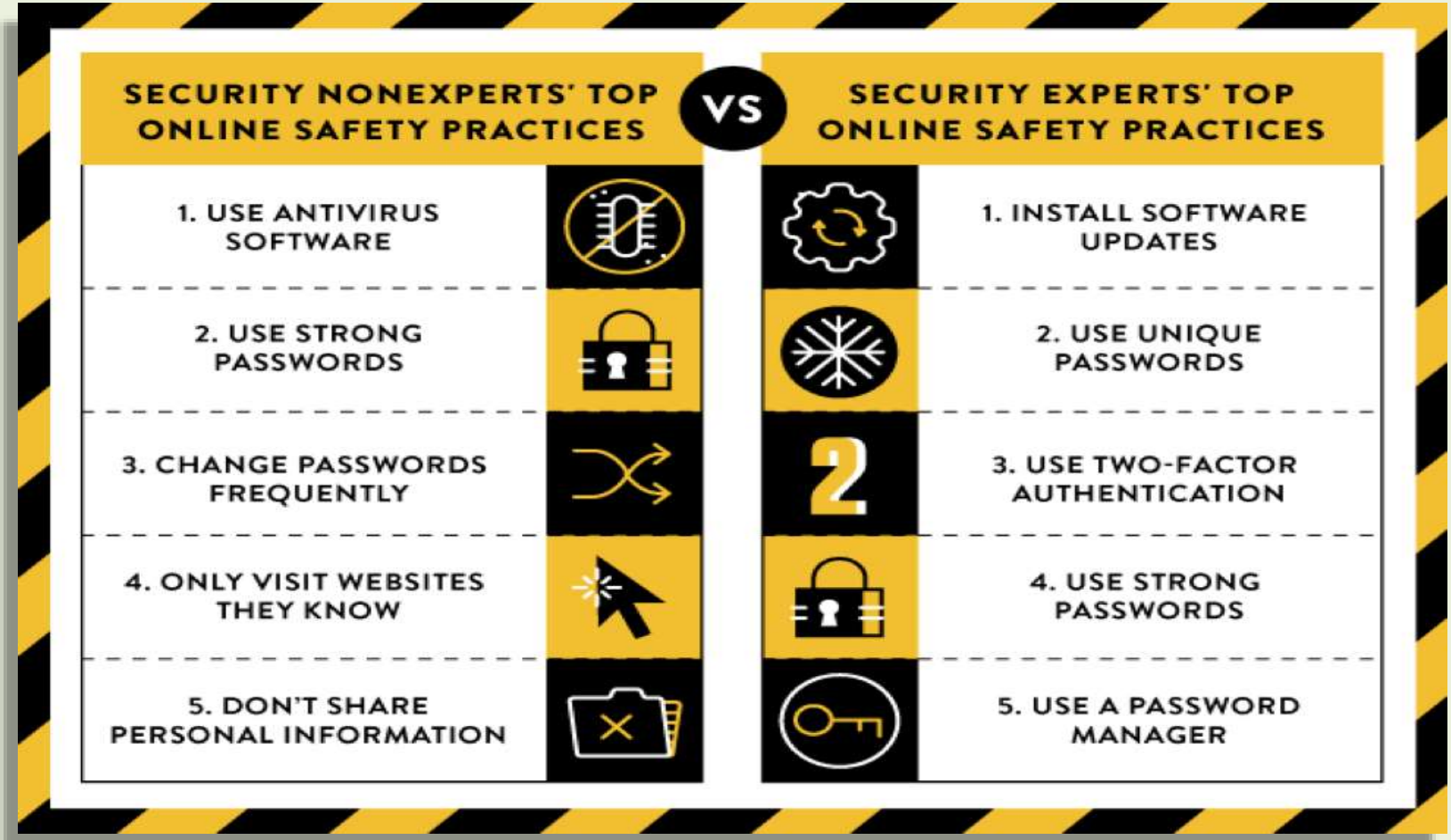
- **Cyber hygiene is often compared to personal hygiene**. Much like an individual engages in certain personal hygiene practices to maintain good health and well-being, cyber hygiene practices can keep data safe and well-protected.
- **In turn, this aids in maintaining properly functioning devices by protecting them from outside attacks**, such as malware, which can hinder functionality.
- **Cyber hygiene relates to the practices and precautions users take with the aim of keeping sensitive data organized**, safe, and secure from theft and outside attacks.

Cyber Hygiene

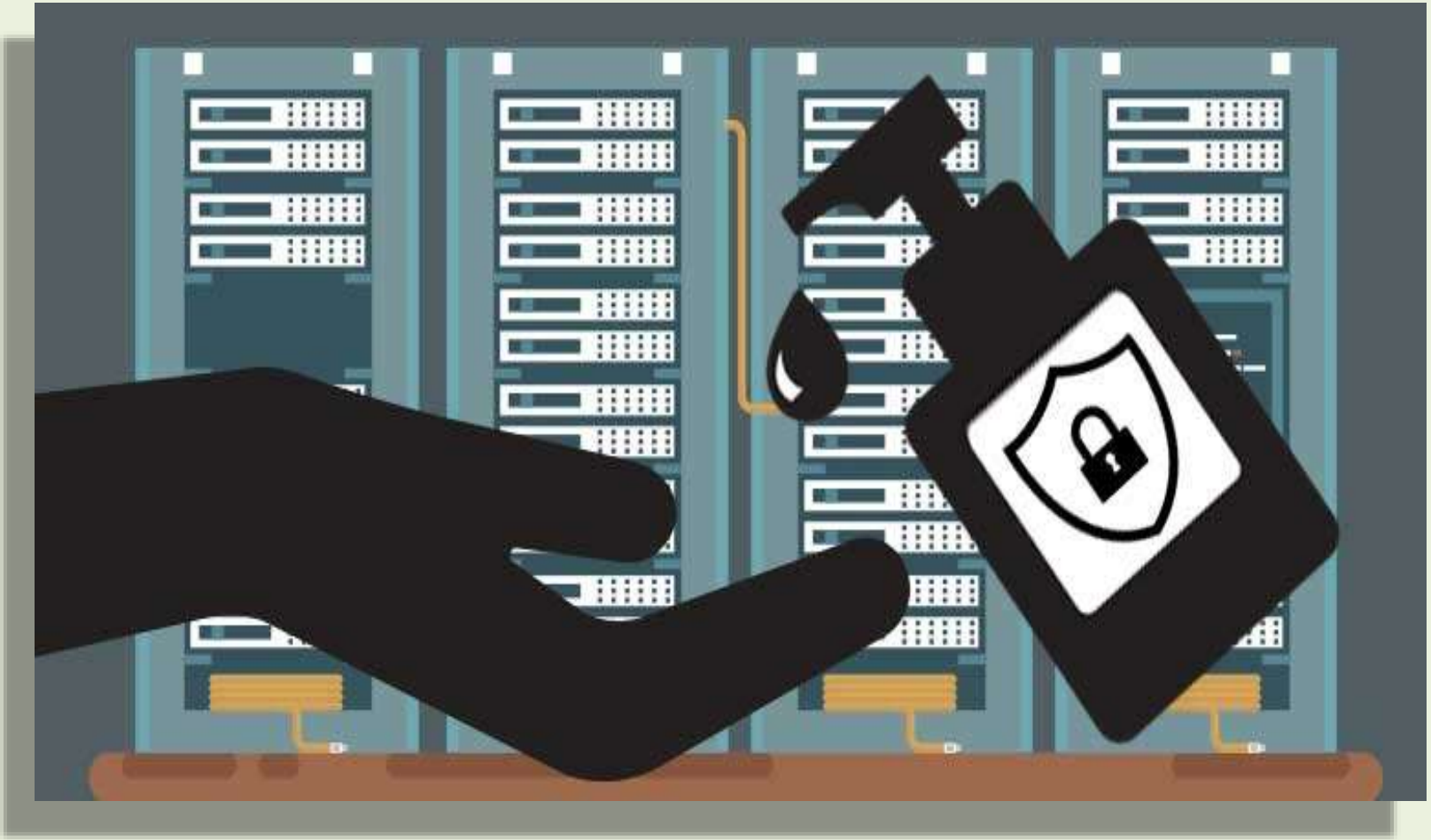
Definition of Cyber Hygiene

- **Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health** and improve online security.
- These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.
- **Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.**

Cyber Hygiene



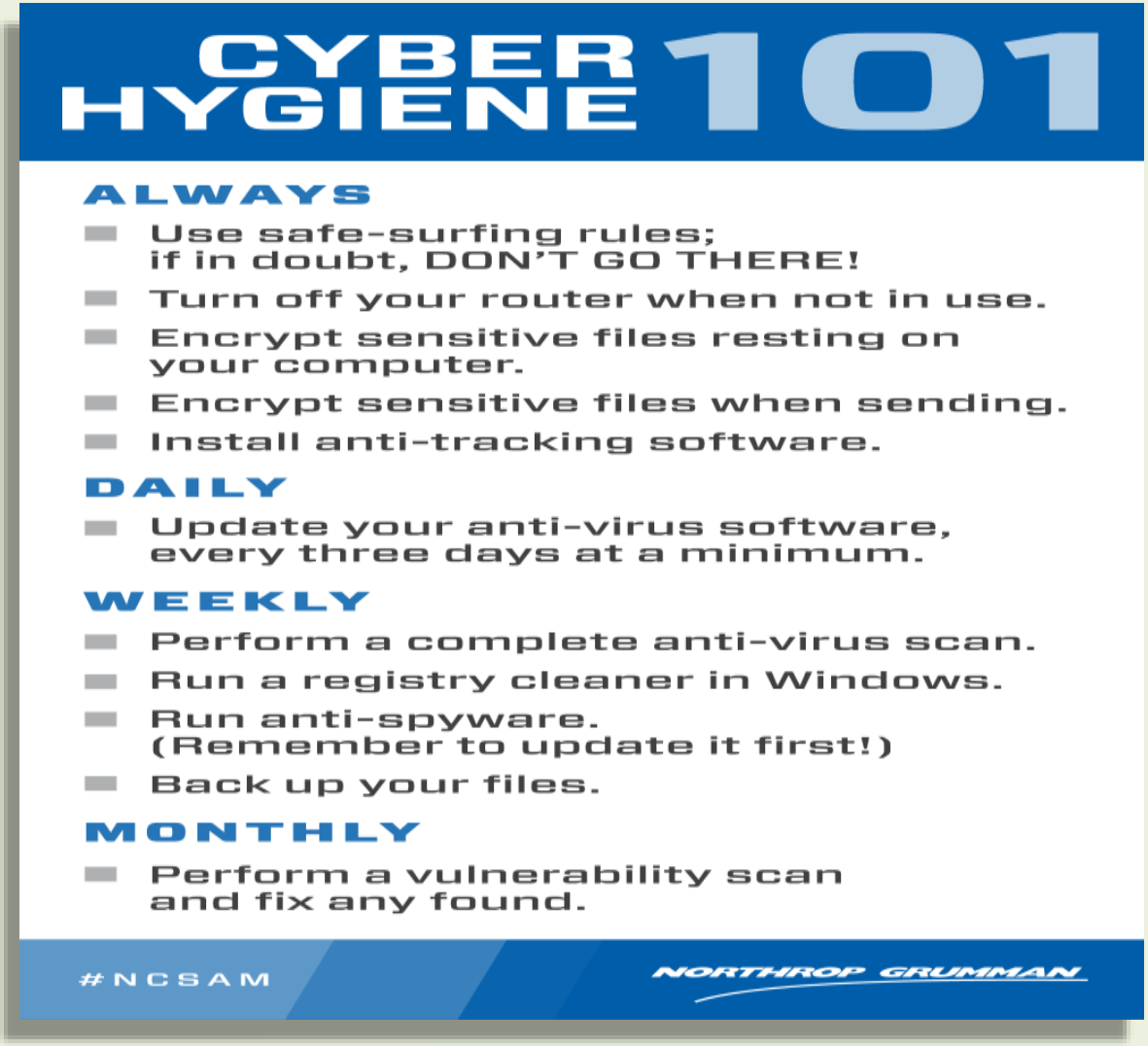
Cyber Hygiene



Benefits of Cyber Hygiene

- **Having a routine cyber hygiene procedure in place for your computers and software is beneficial for two distinct reasons – maintenance and security.**
- **Maintenance is necessary for computers** and software to run at peak efficiency.
- Files become fragmented and programs become outdated, increasing the risk of vulnerabilities.

Benefits of Cyber Hygiene



Benefits of Cyber Hygiene

- Routines that include maintenance are likely to spot many of these issues early and prevent serious issues from occurring.
- **A system that is well-maintained is less likely to be vulnerable to cybersecurity risks.**
- Security is perhaps the most important reason to incorporate a cyber hygiene routine.
- **Hackers, identity thieves, advanced viruses, and intelligent malware are all part of the hostile threat landscape.**
- While predicting threats can be challenging, preparing and preventing them becomes feasible with sound cyber hygiene practices.

Cyber Hygiene

Common Cyber Hygiene Problems

- **Enterprises often have multiple elements in need of cyber hygiene.**
- All hardware (computers, phones, connected devices), software programs, and online applications used should be included in a regular, ongoing maintenance program.
- **Each of these systems have specific vulnerabilities that can lead to different problems.** Some of these problems include:

Common Cyber Hygiene Problems

- **Loss of Data**: **Hard drives and online cloud storage that isn't backed up or maintained is vulnerable to hacking**, corruption, and other problems that could result in the loss of information.
- **Misplaced Data**: **Poor cyber hygiene could mean losing data in other ways. The information may not be corrupted or gone for good, but with so many places to store data**, misplacing files is becoming increasingly commonplace in the modern enterprise.

Common Cyber Hygiene Problems

Common Cyber Hygiene Problems

- **Security Breach: There are constant and immediate threats to all enterprise data. Phishing**, hackers, malware, spam, viruses, and a variety of other threats exist in the modern threat landscape, which is constantly in a state of flux.
- **Out of Date Software: Software applications should be updated regularly, ensuring that the latest security patches and most current versions are in use across the enterprise – for all applications.**

  Out of date software is more vulnerable to attacks and malware.

Common Cyber Hygiene Problems

Common Cyber Hygiene Problems

- **Older Security Software: Antivirus software and other security software must be updated continuously to keep pace with the ever-changing threat landscape.**

  Outdated security software – even software that has gone a few months without an update – can't protect the enterprise against the latest threats.

Common Cyber Hygiene Problems

Best Practices: A Cyber Hygiene Checklist

- **While there are numerous threats and multiple vulnerabilities with each piece of the digital puzzle, creating a cyber hygiene routine isn't as difficult as it may seem.**
- **A few key practices implemented regularly can dramatically improve** the security of any system.

Best Practices: A Cyber Hygiene Checklist

Document All Current Equipment and Programs

- **All hardware, software, and online applications will need to be documented**. Start by creating a list of these three components:
- **Hardware: Computers, connected devices (i.e. printers, fax machines), and mobile devices (i.e. smartphones, tablets).**
  Software: All programs, used by everyone on a particular network, that are installed directly onto computers.
  Applications: Web apps (i.e. Dropbox, Google Drive), applications on phones and tablets, and any other program that isn't directly installed on devices.

Best Practices: A Cyber Hygiene Checklist

Analyze the List of Equipment and Programs

- **After creating a comprehensive list of all cyber-facing components, you can begin to scrutinize the list and find vulnerabilities.**
- **Unused equipment should be wiped and disposed of properly.**
- **Software and apps that are not current should be updated and all user passwords should be changed. If the programs aren't in regular use, they should be properly uninstalled.**
- Certain software programs and apps should be chosen to be the dedicated choice for certain functions for all users. For instance, if both Google Drive and Dropbox are being used for file storage, one should be deemed primary and the other used as backup or deleted.

Best Practices: A Cyber Hygiene Checklist

Create A Common Cyber Hygiene Policy

- **The newly clarified network of devices and programs will need a common set of practices to maintain cyber hygiene**.
- **If there are multiple users, these practices should be documented into a set policy** to be followed by all who have access to the network.
- Here are typical items that should be included into a cyber hygiene policy:

Create A Common Cyber Hygiene Policy

Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

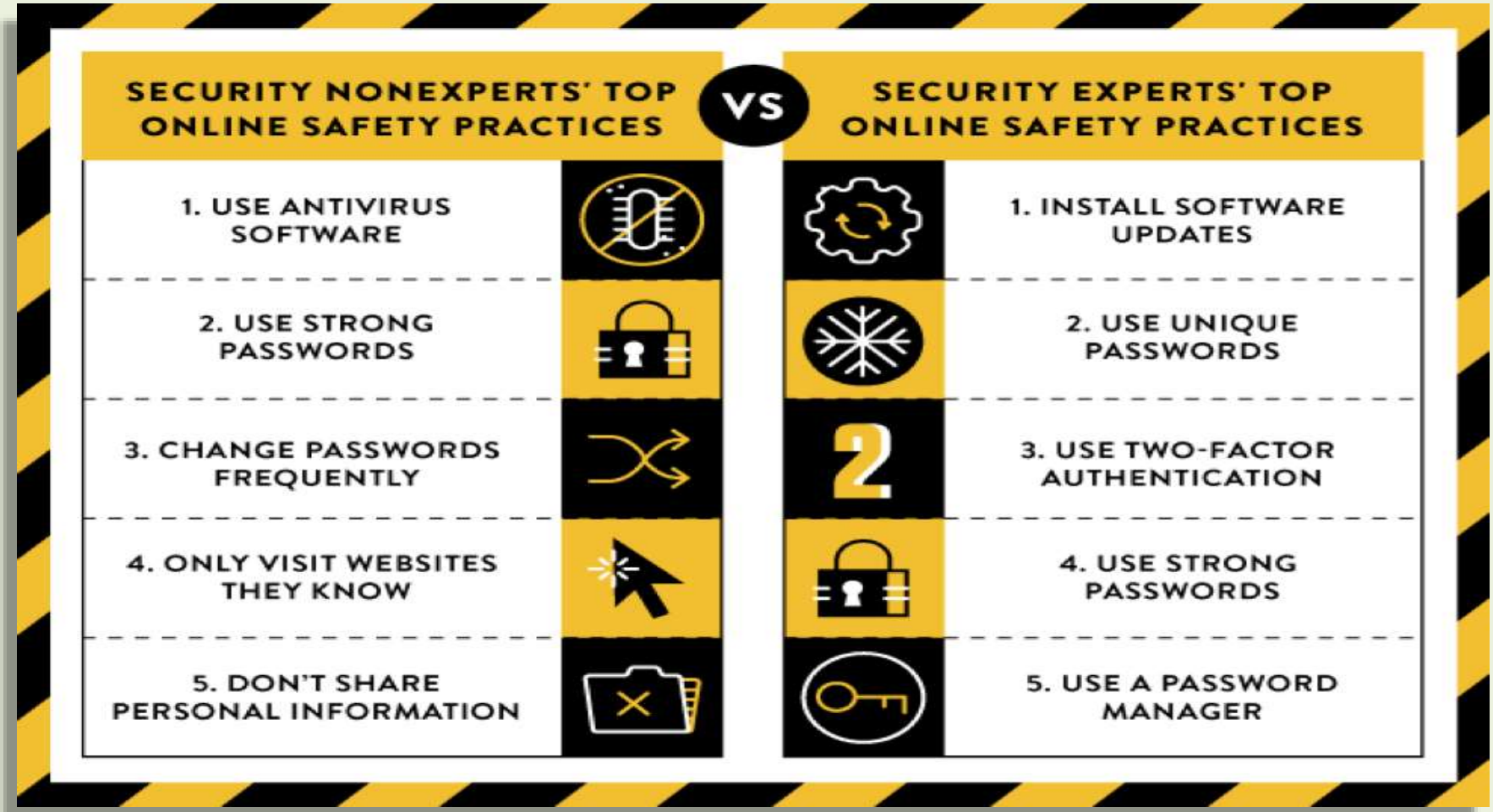
1. Identify and prioritize key organizational services, products, and their supporting assets.
2. Identify, prioritize, and respond to risks to the organization's key services and products.
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
9. Prevent and monitor malware exposures.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Source:

Create A Common Cyber Hygiene Policy

- **Password Changes**: Complex passwords changed regularly can prevent many malicious activities and protect cyber security.
- **Software Updates**: Updating the software you use, or perhaps getting better versions should be a part of your regular hygienic review.
- **Hardware Updates:** Older computers and smartphones may need to be updated to maintain performance and prevent issues

Create A Common Cyber Hygiene Policy



Create A Common Cyber Hygiene Policy

- **Manage New Installs:** Every new install should be done properly and documented to keep an updated inventory of all hardware and software.
- **Limit Users:** Only those who need admin-level access to programs should have access. Other users should have limited capabilities.
- **Back Up Data**: All data should be backed up to a secondary source (i.e. hard drive, cloud storage). This will ensure its safety in the event of a breach or malfunction.
- **Employ a Cyber** Security Framework: Businesses may want to review and implement a more advanced system (e.g. the NIST framework) to ensure security.

Create A Common Cyber Hygiene Policy

Humans in the Loop: Cyber Hygiene

- Use email securely
- Identify phishing
- Change passwords (make them complex)
- Practice wireless security
- Understand social engineering
- Use social media judiciously
- Be alert to insider threats
- Secure the supply chain

Create A Common Cyber Hygiene Policy

- **Once the policy is created, the routine for each item should be set to appropriate timeframes**.
- For instance, changing passwords every 30 days or check for updates at least once per week could be set in place.
- **Doing so will ensure the continued cyber hygiene of your entire network of hardware and software.**

Create A Common Cyber Hygiene Policy

Create A Common Cyber Hygiene Policy

- **Developing comprehensive cyber hygiene procedures is a must for today's enterprises**. When carried out in conjunction with robust, enterprise-wide security practices, sound cyber **hygiene practices aid in maintaining a sound security posture for modern organizations.**

CYBER HYGIENE 101

ALWAYS

- Use safe-surfing rules; if in doubt, DON'T GO THERE!
- Turn off your router when not in use.
- Encrypt sensitive files resting on your computer.
- Encrypt sensitive files when sending.
- Install anti-tracking software.

DAILY

- Update your anti-virus software, every three days at a minimum.

WEEKLY

- Perform a complete anti-virus scan.
- Run a registry cleaner in Windows.
- Run anti-spyware. (Remember to update it first!)
- Back up your files.

MONTHLY

- Perform a vulnerability scan and fix any found.

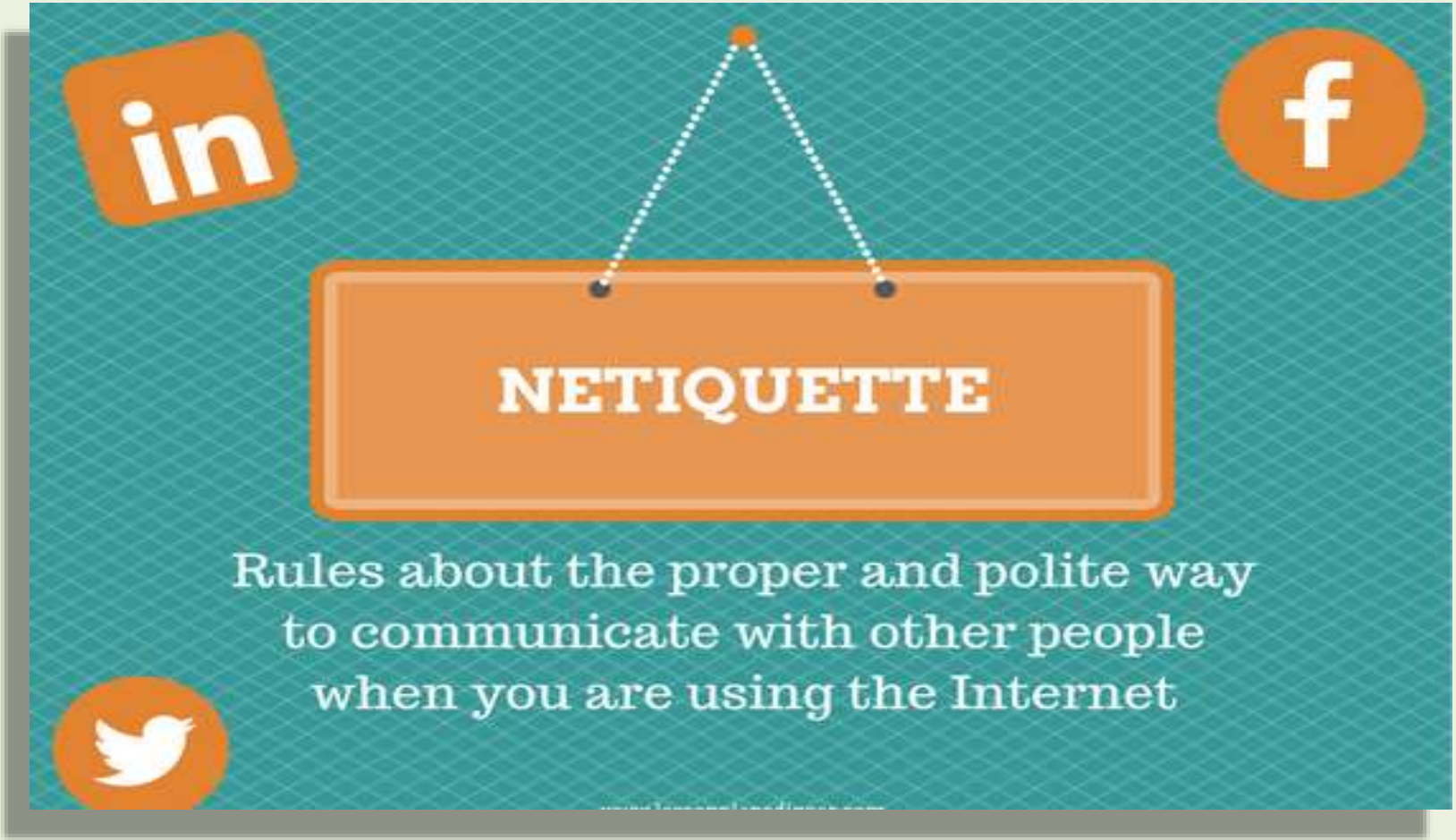
#NCSAM

NORTHROP GRUMMAN

Golden Rules Of Netiquette

- **What is Netiquette?**
- Simply stated, it's network etiquette -- that is, the etiquette of cyberspace."
- **In other words, Netiquette is a set of rules for behaving properly online.**

Golden Rules Of Netiquette



Golden Rules Of Netiquette

- **Rule 1: Remember the human**
- The golden rule your parents and your kindergarten teacher taught you was pretty simple:
- Do unto others as you'd have others do unto you. Imagine how you'd feel if you were in the other person's shoes. **Stand up for yourself, but try not to hurt people's feelings.**

Golden Rules Of Netiquette

Golden Rules Of Netiquette

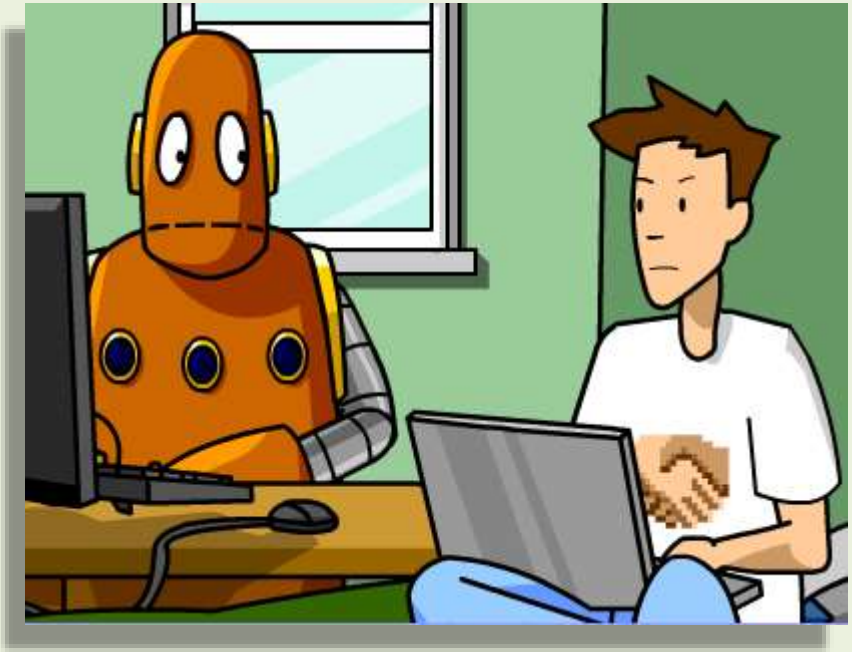
- **Rule 2: Adhere to the same standards of behavior online that you follow in real life**
- **In real life, most people are fairly law-abiding, either by disposition or because we're afraid of getting caught. In cyberspace**, the chances of getting caught sometimes seem slim. And, perhaps because people sometimes forget that there's a human being on the other side of the computer, some people think that a lower standard of ethics or personal behavior is acceptable in cyberspace.
- **The confusion may be understandable, but these people are mistaken. Standards of behavior may be different in some areas of cyberspace, but they are not lower than in real life.**

Golden Rules Of Netiquette

Rule 3: Know where you are in cyberspace

- **What's perfectly acceptable in one area may be dreadfully rude in another**. For example, in most TV discussion groups, passing on idle gossip is perfectly permissible.
- **But throwing around unsubstantiated rumors in a journalists' mailing list will make you very unpopular there.**
- And because Netiquette is different in different places, it's important to know where you are. Thus the next corollary:
- ***Lurk before you leap***
- When you enter a domain of cyberspace that's new to you, take a look around. Spend a while listening to the chat or reading the archives. Get a sense of how the people who are already there act. Then go ahead and participate.

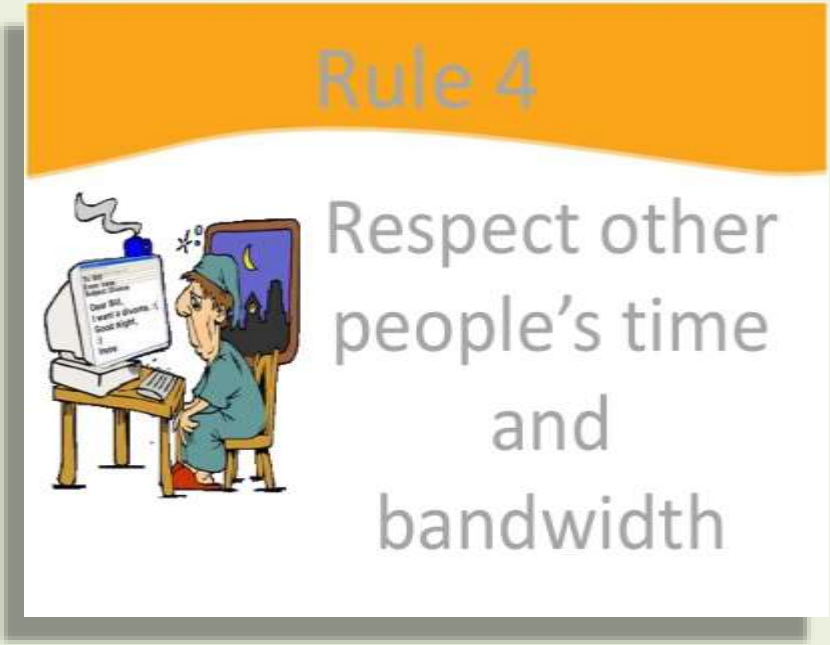
Rule 3: Know where you are in cyberspace



Rule 4: Respect other people's time and bandwidth

- **Rule 4: Respect other people's time and bandwidth**
- Bandwidth is the information-carrying capacity of the wires and channels that connect everyone in cyberspace.
- **There's a limit to the amount of data that any piece of wiring can carry at any given moment -- even a state-of-the-art fiber-optic cable.**
- The word "bandwidth" is also sometimes used to refer to the storage capacity of a host system.
- **When you accidentally post the same note to the same newsgroup five times, you are wasting both time (of the people who check all five copies of the posting) and bandwidth (by sending repetitive information over the wires and requiring it to be stored somewhere).**

Rule 4: Respect other people's time and bandwidth



Rule 5: Make yourself look good online

- **Rule 5: Make yourself look good online**
- *Take advantage of your anonymity*
- I don't want to give the impression that the net is a cold, cruel place full of people who just can't wait to insult each other.
- *Know what you're talking about and make sense*
- Pay attention to the content of your writing. Be sure you know what you're talking about
- *Don't post flame-bait*
- Finally, be pleasant and polite. Don't use offensive language, and don't be confrontational for the sake of confrontation.

Rule 5: Make yourself look good online

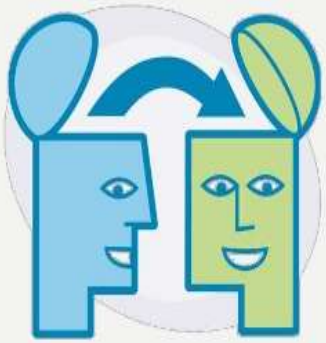
Rule 6: Share expert knowledge

- **Rule 6: Share expert knowledge**
- The strength of cyberspace is in its numbers.
- **The reason asking questions online works is that a lot of knowledgeable people are reading the questions.**
- And if even a few of them offer intelligent answers, the sum total of world knowledge increases. The Internet itself was founded and grew because scientists wanted to share information. Gradually, the rest of us got in on the act.
- **So do your part.**

Rule 6: Share expert knowledge

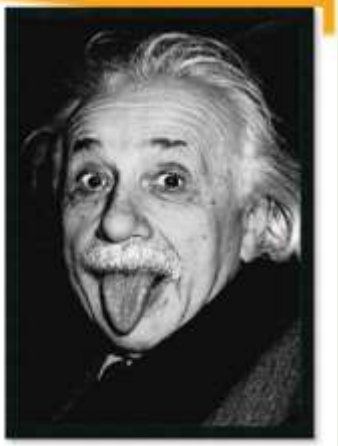
RULE 6: SHARE EXPERT KNOWLEDGE.

- Ask questions online.
- Share what you know online.
- Post the answers to your questions online because someone may have the same question you do.



Rule 6

Share
Expert
Knowledge



Rule 7: Help keep flame wars under control

- **Rule 7: Help keep flame wars under control**
- "Flaming" is what people do when they express a strongly held opinion without holding back any emotion. It's the kind of message that makes people respond, "Oh come on, tell us how you really feel." Tact is not its objective.
- Flames can be lots of fun, both to write and to read. And the recipients of flames sometimes deserve the heat.
- But Netiquette does forbid the perpetuation of flame wars

Rule 7: Help keep flame wars under control

Some joker is going to get well and truly flamed

Rule 8: Respect other people's privacy

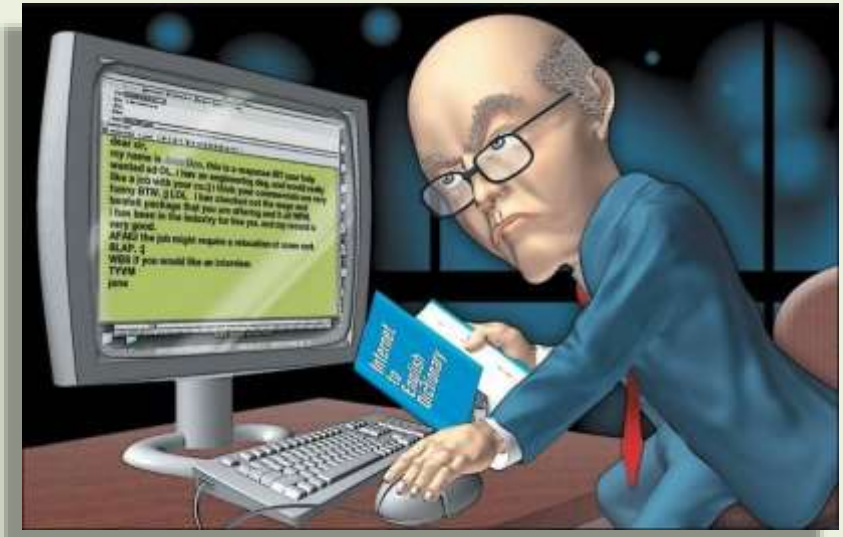
- **Rule 8: Respect other people's privacy**
- Of course, you'd never dream of going through your colleagues' desk drawers. So naturally you wouldn't read their email either.
- Unfortunately, a lot of people would.

Rule 8: Respect other people's privacy

Rule 9: Don't abuse your power

- **Rule 9: Don't abuse your power**
- **Some people in cyberspace have more power than others.**
- **There are wizards in MUDs (multi-user dungeons), experts in every office, and system administrators in every system.**
- Knowing more than others, or having more power than they do, does not give you the right to take advantage of them. For example, sysadmins should never read private email.

Rule 9: Don't abuse your power



Rule 10: Be forgiving of other people's mistakes

- **Rule 10: Be forgiving of other people's mistakes**
- **Everyone was a network newbie once.** So when someone makes a mistake -- whether it's a spelling error or a spelling flame, a stupid question or an unnecessarily long answer -- be kind about it. If it's a minor error, you may not need to say anything. **Even if you feel strongly about it, think twice before reacting. Having good manners yourself doesn't give you license to correct everyone else.**
- **If you do decide to inform someone of a mistake, point it out politely, and preferably by private email rather than in public. Give people the benefit of the doubt; assume they just don't know any better. And never be arrogant or self-righteous about it.**

Rule 10: Be forgiving of other people's mistakes

Terminology

- **Phishing**
- Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication

Terminology

- **Malware**
- **Malware**, or malicious software, is any program or file that is harmful to a computer user. **Malware** includes computer viruses, worms, Trojan horses and spyware.

Terminology

- **Ransomware**
- a type of malicious software designed to block access to a computer system until a sum of money is paid.

Terminology

- **Hacking**
- Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

Terminology

- **Cookies**
- **Cookie** (also called web **cookie**, Internet **cookie**, browser **cookie**, or simply **cookie**) is a small piece of data sent from a website and stored on the user's **computer** by the user's web browser while the user is browsing.

Terminology

- **Antivirus**
- **software designed to detect and destroy computer viruses.**

References

- **Cyber Hygiene: 11 Essential Practices**
- **https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html**
- **Good Cyber Hygiene**
- **https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html**
- **How Cyber Hygiene Can Protect Against Cyberattacks**
- **https://insights.leidos.com/competencies/how-cyber-hygiene-can-protect-against-cyberattacks.**
- **Netiquette and Online Ethics: What Are They?**
- **https://www.webroot.com/in/en/home/resources/tips/ethics-and-legal/ethics-netiquette-and-online-ethics-what-are-they**
- **Netiquette: Rules of Behavior on the Internet**
- **https://www.education.com/reference/article/netiquette-rules-behavior-internet/**
- **What is Cyber Hygiene?**
- **https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more**

Thanks…

GHT