AES CYBER NINJA

Educate. Enable. Empower.

– Cyber Ninja Guide –

VERSION 2

AES CYBER NINJA

Educate. Enable. Empower.

"Cybersecurity is an issue of safety that starts with our people. As AES people, we must put safety first when leveraging the power of the Internet both at work and at home. The following guidelines will educate, enable and empower our people and contractors to use these resources safely while playing an active role in protecting AES, ourselves and our families from the growing risks of being connected."

Scott P Goodhart

Scott Goodhart
Vice President and CISO

CYBERSAFETY AT WORK

CYBERSAFETY OUTSIDE THE OFFICE

WHAT TO DO

Work

CYBERSAFETY WHEN WORKING IN THE FIELD OR IN AES FACILITIES

Empowering our people is our first line of defense.

PASSWORDS: YOUR FIRST LINE OF DEFENSE

80%
of cyberattacks involve weak passwords

55%
of people use one password for all logins

- Use both lowercase and capital letters, as well as a combination of letters, numbers and special characters.
- Use words or phrases that cannot be found in any dictionary of any language.
- Do not use passwords that are based on personal information that can be easily guessed (such as your birthdate, telephone number, or the name of your spouse, child or pet).
- Use different passwords on different systems or websites.
- Change your password on a regular basis.
- Do not share your password with anyone else.
- Do not write your password down and leave it in your desk or next to your computer.

DAILY TIPS FOR INFORMATION PROTECTION

These simple, daily tasks require very little effort, but they significantly reduce the likelihood of confidential information being stolen from AES.

- Be sure to lock your computer when you walk away from it, even if you will only be gone for a short period of time.
- Do not leave your mobile devices unattended since having physical access to a device makes it easier for an attacker to break into it.
- Store your documents on AES network drives so information is backed up and available for disaster recovery purposes. Avoid storing AES documents on personal cloud repositories, such as Box, Dropbox and Google Drive.

At the end of each day...

- Ensure that confidential or sensitive documents are removed from your desk and printers before leaving for the day.
- Remember to shred or properly destroy these documents when they are no longer needed.
- For both security and business resilience purposes, take your computer and mobile devices home each night.

THINK BEFORE YOU CLICK

Malicious links are one of today's biggest cybersecurity threats. Slow down and remember these guidelines before you click.

- If it sounds too good to be true, it probably is. Don't click any suspicious links.
- Hover over links contained in messages and make sure they direct you to the correct website.
- Pay attention to the email address of a sender to ensure it is legitimate.
- Avoid downloading free software (especially those displayed in pop-up ads), which is a frequent source of viruses.
- Be suspicious of threatening or unnecessarily urgent emails.
- If you receive an email or instant message from a business contact that seems unusual or does not sound like something they would typically say, contact them through another means of communication and ask them if they actually sent the message before opening it.
- Avoid clicking on links, pictures and videos with catchy phrases such as "funniest ever" or "you have got to see this."

156 MILLION

PHISHING EMAILS ARE SENT GLOBALLY EVERY DAY

- Do not provide personal information or information about AES unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

If you receive any email messages that appear "fishy", please click on the "Report Phishing" icon ( ) on your Outlook toolbar and the email will be sent to your local IT team for analysis.

CYBERSAFETY ON SOCIAL MEDIA

ABOUT **10%**

of **ALL SOCIAL MEDIA USERS** have received a **CYBER THREAT.**

More than **600,000** accounts are **COMPROMISED** **EVERY DAY on Facebook ALONE**

1 3

of **data breaches** ORIGINATED via social networks

- Exercise caution when posting personal information that may make you or your family vulnerable, such as your address or information about your schedule, routine or vacation plans.
- Also, if your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing.
- Be wary of out-of-context connection requests. Since creating a social media account only requires a valid email address, it is easy for hackers to impersonate anyone online.
- Take advantage of social media site privacy settings to limit the information you make available to friends of friends or the public.

TIPS FOR THE SAFE USE OF USB DRIVES

All of the characteristics of USB drives and other removable media devices that make them so convenient (small, readily available and portable) also make them targets for hackers.

- Do not connect personally-owned USB drives to AES computers.
- Likewise, do not connect USB drives issued by AES to personally-owned computers.
- If you find a USB drive on the floor, in an elevator or at a coffee shop nearby your facility, retrieve the device, deliver it to your local IT team and inform them of its suspicious origin.
- Always physically secure any USB drives containing confidential information while on or off AES premises.
- When possible, use passwords and encryption features available on USB drives to further protect your information.

Home & Travel

CYBERSAFETY WHEN WORKING OUTSIDE THE OFFICE OR TRAVELING

The majority of the previous cybersafety tips still apply when traveling, working from home or working from other locations outside of an AES facility. The following pages contain additional precautions to take when offsite.

SAFETY TIPS WHEN WORKING OUTSIDE THE OFFICE OR TRAVELING

- Always use VPN when out of the office.
- Avoid performing AES work on non-AES computers.
- Also, refrain from exchanging files between non-AES computers and AES-issued devices.
- Do your best to avoid open, unsecured Wi-Fi networks (such as those in hotels, airports, airplanes and coffee shops) to conduct personal or professional business. If there is no alternative, use VPN to establish an encrypted connection.
- Use a privacy screen. Be aware of people nearby, who may be reading over your shoulder or shoulder surfing to gain access to AES proprietary or your personal information.
- Refrain from using your AES email address/AES credentials for personal account creation on e-commerce, media and blog sites.

Home & Travel

MOBILE DEVICE AND APPLICATION SECURITY

As more and more people rely on smartphones to conduct business and carry out everyday responsibilities, these devices are becoming more and more valuable as targets for cyberattack.

- Protect your portable devices such as your smartphone and tablet. Never leave these devices unattended in a public space such as in a coffee shop, hotel or airport.
- Enable password security on all of your devices, and select passwords that are difficult for others to guess. That way, if your mobile device is lost or stolen, it will be more difficult for an attacker to gain access to your information.
- Only purchase or download necessary applications from official app stores, such as Apple App Store or Google Play.
- Just like you would with your PC, keep your smartphone's software up to date. Mobile phone software and network services have vulnerabilities, just like their PC counterparts do.
- Only use electrical outlets to recharge your mobile devices. Avoid connecting your devices to a public charging station that requires connection to a computer via USB.

What if?

WHAT TO DO IF MY DEVICE IS LOST OR STOLEN?

If one of your devices is lost or stolen, please notify your manager and your local IT team immediately.

WHAT TO DO IF MY DEVICE IS COMPROMISED?

Here are a few signs that your computer may be infected with a virus:

- You receive a virus notification message from the anti-virus software on your computer.
- You notice strange behavior from your computer, such as programs starting unexpectedly.
- Your colleagues or friends inform you that they have received seemingly unusual email messages from your address.
- Your computer freezes or hangs frequently or programs start running slowly.
- You notice that files or folders have been deleted or changed.

If you notice one of these warning signs, please take these two steps immediately:

- Disconnect your computer from the network to prevent the virus from spreading.
- Contact the Arlington Connection Corner for assistance with removing the virus.

AES CYBER NINJA

Educate. Enable. Empower.

To learn more about becoming a Cyber Ninja, please contact your local Cybersecurity team.

1/2016

CYBER SIX
TOP SAFETY TIPS

1. SELECT STRONG PASSWORDS

Hackers have many tools available to crack passwords, but you can make it more difficult by selecting strong passwords, changing them regularly and keeping them confidential.

2. THINK BEFORE YOU CLICK

If anything about an email, IM or website seems suspicious, do not click on links, download files or open attachments.

3. USE SECURE CONNECTIONS

When connecting to the Internet outside of the office, use VPN to protect your information.

4. BE CAUTIOUS WHEN USING USB DRIVES

Avoid the use of USB drives and other removable media unless you are certain that the source is trustworthy.

5. EXERCISE DISCRETION WHEN USING SOCIAL MEDIA

Be aware that information you share on social media sites can be compiled and then used against you in highly personal and realistic cyberattacks.

6. YOU WILL BE COMPROMISED SO BE PREPARED

In today's cyber age, compromise is inevitable. Know the warning signs and report incidents immediately.

AES

we are the energy