DON’T GET HOOKED

BEWARE OF PHISHING SCAMS

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity. © 2019 by Schweitzer Engineering Laboratories, Inc. • LMD0382-01 • 20190415
PRACTICE SECURITY IN DEPTH

The best cybersecurity has many layers.
The best cybersecurity has many layers.
ATTACKERS ARE LOOKING

Never expose critical infrastructure to the internet.
Isolate critical infrastructure environments.
BE SUSPICIOUS OF EVERYTHING
(in a nonparanoid fashion)

Cyber criminals make the Internet a dangerous place. Be street-smart. Keep a critical eye out, and avoid unsafe activities.
YOUR COMPUTER IS A BUSINESS TOOL

The more casual your web use, the greater your risk of a malware infection.
DON'T USE DEFAULT PASSWORDS

INSTEAD, SHOW SOME CREATIVITY!

SherlockOHMS+watTs0n

Make your password as unique as you are. A phrase is a great way to create a strong password that’s easy to remember and hard to crack.
CONFIRM THE SOURCE

Never click on unexpected email links or attachments.
DO YOU KNOW WHO YOUR DEVICES ARE TALKING TO?

Protect your critical infrastructure with secure communications.
ARE DIGITAL DOORS LEFT OPEN?

Securing the substation means more than locking the gate. Make sure you close your digital doors.

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.
© 2019 by Schweitzer Engineering Laboratories, Inc. • LM00402-01 • 20190219
YOUR DOG'S NAME IS NOT A PASSWORD

Choose a password that is easy to remember, yet hard to guess.
DON'T OPERATE THE POWER SYSTEM FROM YOUR HOME

Critical jobs require a secure environment. Keep the Internet out to keep your system from being compromised.
ELECTRICITY IS POWERFUL, INVISIBLE, AND DANGEROUS

SO IS INFORMATION

Be careful with both.
YOUR FILES HAVE BEEN ENCRYPTED!

...But not by you.

Ransomware is on the rise.
Don't be a victim of extortion.

• Back up data regularly.
• Keep systems up to date.
• Be wary of phishing emails.
• Avoid risky online behavior.
KNOW HOW TO HANDLE A LEAK

The time to make a plan is not during or after a crisis. Learn to identify a security incident and how to respond.
KEEP THE INTERNET OUTSIDE THE FENCE

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.

© 2019 by Schweitzer Engineering Laboratories, Inc. • LMO0386-01 • 20190417
KEEP YOUR TOOLS CLEAN

Don't let infections spread. Always scan for malware before using USB sticks.
MULTIFACTOR AUTHENTICATION

It’s like wearing a belt and suspenders.

A strong password is a good start, but it could use an extra layer of protection. Enable multifactor authentication whenever possible to validate that the person signing into your account is really you.
Only share information with those who need to know.

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.

© 2019 by Schweitzer Engineering Laboratories, Inc. • LM00383-01 • 20190415
PAY ATTENTION TO STRANGE BEHAVIOR

Whether by a computer or a person, odd behavior can be a warning sign that something is wrong. Report concerns without delay!

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.
© 2018 by Schweitzer Engineering Laboratories, Inc. • LM00343-01 • 20180223
PATCH YOUR SYSTEMS REGULARLY

Many breaches are based on common exploits. Be aware of the risks, and apply well-tested patches or mitigate vulnerabilities with other security controls.

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.

© 2018 by Schweitzer Engineering Laboratories, Inc. • LM00339-01 • 20180223
Enable multifactor authentication whenever possible to validate that the person signing in to your account is really you.
PATROL YOUR SECURITY PERIMETERS

Promptly report problems or concerns.
USE SECURE BUSINESS PRACTICES

Only use USB drives you know are clean. Establish protocols to keep them isolated and free from malware.
SERIOUSLY

Cyber attacks are real, and critical infrastructure is a major target. Be aware and prepared.
Firewall rules alone can’t recognize every intruder. Whitelist to prevent unwanted access to your critical infrastructure.
YOU WOULDN'T LET A STRANGER DRIVE YOUR CAR

Don’t let strangers into the network. Use whitelisting to protect our systems.
Phishing emails often contain grammatical errors or misspellings. Use caution before clicking on potentially dangerous links or attachments.
Unexpected content, fake links, and odd or unknown sender addresses are indicators that an email might be phishing.
TECHNOLOGY HAS CHANGED

Cyber attacks are more advanced than ever. Practice security in depth.
Unexpected links, attachments, or requests are indicators that an email might be phishing.
THIEVES and ENEMIES LOVE DARKNESS

Keep them out of our power networks to keep the lights on.
UNEXPECTED EMAIL?

Proceed with caution—it could be malicious! Never open email links or unexpected attachments. Check with Security to verify the safety of suspect emails.
TREAT ALL KEYS WITH CARE

Login Freddie_K_OWatt
Password ************A

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity.

© 2019 by Schweitzer Engineering Laboratories, Inc. • LM00387-01 • 20190502
I DON’T SHARE MY TOOTHBRUSH OR MY PASSWORD

Don’t share your passwords, and do change them regularly. Treat your toothbrush the same.
TROUBLE IN DISGUISE

Only share information if you can confirm that the requester is who they claim to be and that they have a need to know.
Phishing scams lure you to click on dangerous links. Don’t become a cyber criminal’s trophy catch.
UNEXPECTED EMAIL?

Proceed with caution—it could be malicious! Never open email links or unexpected attachments. Check with IT to verify the safety of suspect emails.
SEE SOMETHING UNUSUAL?

If you notice something that just doesn’t look right, report it immediately.
The longer the password, the stronger it is. A unique phrase is a great way to create a strong password that’s easy to remember.
WHAT ARE YOU LOOKING AT?

The more casual your web use, the greater your risk of a malware infection.

SEL SCHWEITZER ENGINEERING LABORATORIES

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity
© 2019 by Schweitzer Engineering Laboratories, Inc • LMD0397-01 • 20190219
WHILE SMALL IN SIZE, USB DEVICES CARRY A HUGE RISK

USB malware is more advanced than ever. Don’t get bitten—keep USB devices off of our systems.
WHILE SMALL IN SIZE, USB DEVICES CARRY A HUGE RISK

USB malware is more advanced than ever. Don’t get bitten—only use approved, trusted, and clean devices.

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity. © 2018 by Schweitzer Engineering Laboratories, Inc. • LM00348-01 • 20180223
YOU WOULDN’T SAIL WITHOUT A LIFE JACKET

Just like a life jacket, security controls keep you safe. Tampering with or disabling them can put you at unnecessary risk.
YOU
ARE THE FIRST AND THE LAST DEFENSE

Security tools can’t replace your role in a robust security strategy. Take a stand to know your security policies and apply them.
YOU WOULDN'T DRIVE WITHOUT A SEAT BELT

Just like a seat belt, security controls keep you safe. Reduce your risk by keeping them in place.
WHO?
WHAT?
WHEN?

Confirm who you’re talking to, and only share information they need to know.
WHILE SMALL IN SIZE, USB DEVICES CARRY A HUGE RISK

USB malware is more advanced than ever. Don’t get burned—only use approved, trusted, and clean devices.
USE UNIQUE PASSWORDS

Choose a password that is easy to remember, yet hard to guess. A phrase is a great way to create a strong password that’s easy to remember.