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.
Enable multifactor authentication whenever possible to validate that the person signing in to your account is really you.
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.
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.
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. • LMD0339-01 • 20180223
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.
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.
IS YOUR PRIVATE INFORMATION AS PUBLIC AS THIS POSTER?

Protect Yourself on Social Media

• Use a strong password and multifactor authentication.
• Tune your privacy settings.
• Only share what you would risk the entire world seeing.
• Be on guard for malicious messages from scammers or hijacked accounts.

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity
© 2018 by Schweitzer Engineering Laboratories, Inc. - LM00342-01-20180223
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!
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 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.
YOU WOULDN’T DRIVE WITHOUT A SEAT BELT

Just like a seat belt, security controls keep you safe. Tampering with or disabling them can put you at unnecessary risk.
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.

 SEL SCHWEITZER ENGINEERING LABORATORIES

For information about SEL cybersecurity solutions or copies of this poster, visit selinc.com/cybersecurity
© 2018 by Schweitzer Engineering Laboratories, Inc. • LMD0347-01 • 20180223
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.
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.
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.
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.
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.
USE STRONG PASSWORDS

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.
THERE'S MORE TO SECURING THE SUBSTATION THAN LOCKING THE GATE

Did you leave any digital doors open?
He wouldn’t operate from his home.

DON’T OPERATE THE POWER SYSTEM FROM YOUR HOME.

Critical jobs require a sterile environment. Keep the Internet out to keep your system from infection.
DO NOT TRY THIS AT HOME

Don't operate the power system from your home. Critical jobs require a sterile environment. Keep the Internet out to keep your system free from infection.

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

© 2015 by Schweitzer Engineering Laboratories, Inc. • LM00285-01 • 20151105
Good. The gate’s locked.

Are digital doors still open?
KEEP THE INTERNET OUTSIDE THE FENCE
Isolate critical infrastructure environments.
DO YOU KNOW WHO YOUR DEVICES ARE TALKING TO?

Protect your critical infrastructure by securing their communications.

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
© 2015 by Schweitzer Engineering Laboratories, Inc. - LM00289-01 - 20151105
WHITELIST ACCESS TO PROTECT YOUR SYSTEMS

Firewall rules alone can't recognize every wolf. Whitelist to prevent unwanted access to your critical infrastructure.
Do You Know Who Your Devices Are Talking To?

KEEP LOGS AND MONITOR YOUR NETWORK TRAFFIC TO ENSURE YOUR SYSTEM IS KEEPING GOOD COMPANY.
ELECTRICITY is powerful, invisible, and dangerous.

So is INFORMATION.

BE CAREFUL WITH BOTH!
You Wouldn’t Let a Stranger Drive Your Car

Don’t let one operate our power system!

WHITELIST ACCESS TO PROTECT OUR SYSTEMS.
ATTACKERS ARE LOOKING.

CONCEAL YOUR ACCESS TOOLS.

Never expose critical infrastructure to the Internet.
THIEVES and ENEMIES LOVE DARKNESS

Keep them out of our power networks to keep the lights on.
YOUR COMPUTER IS A BUSINESS TOOL

The more casual your web use, the greater your risk of a malware infection.
ANATOMY OF A PHISHING ATTACK

- **Sender Address Can Be Spoofed**
- **Reply Address Is Different From Sender Address**
- **Links Don’t Match the Text of the Link**
- **Indicates Urgency**
- **Looks Genuine**
- **Odd Or Doesn’t Make Sense**
- **Often Has Spelling Or Grammatical Errors**
- **Contains Dangerous Link Or Attachment**

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity
© 2014 by Schweitzer Engineering Laboratories, Inc. · LM00246-01 · 20160613
SEE SOMETHING UNUSUAL?

IF YOU NOTICE SOMETHING THAT JUST DOESN’T LOOK RIGHT, REPORT IT IMMEDIATELY AT:

© 2014 by Schweitzer Engineering Laboratories, Inc. · LM00245-01 · 20140613
DON’T GET CAUGHT

Phishing email scams lure people into clicking on dangerous links. Take an extra second to examine the email so you don’t become a cyber criminal’s trophy catch.
Cyber attacks are real, and critical infrastructure is a major target. Be aware and prepared.
WHO?
WHAT?
WHEN?

Not all information is meant to be shared. Confirm who you’re talking to and if you’re sharing information they need to know.
The more casual your web use, the greater your risk of a malware infection.
WHAT ARE YOU LOOKING AT?

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

If something looks suspicious, report it immediately at:
Phishing emails often contain grammatical errors or misspellings. Use caution before clicking on potentially dangerous links or attachments.
START HERE

Did you just receive an email?

NO

Come back when you do.

YES

Excellent. Were you expecting it?

NO

Does it contain any links or attachments?

YES

Anything weird or unusual?

NO

Does it look genuine?

NO

Are there any spelling or grammar errors?

YES

Never click on email links or attachments in unexpected emails. Check with IT if you are unsure.

NO

Great! The email is probably safe.

YES

Time to be highly skeptical!!

Do you recognize the sender?

NO

That means nothing! The sender address can be easily spoofed.

YES

TO CLICK OR NOT TO CLICK

An engineer’s guide to reading email.

© 2014 by Schweitzer Engineering Laboratories, Inc. · LM00237-01 · 20140613
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.
Unexpected content, fake links, and odd or unknown sender addresses are indicators that an email might be phishing.
Unexpected content, fake links, and odd or unknown sender addresses are indicators that an email might be phishing.
Today’s cybercriminals combine advanced technology with social tactics to steal information.

Validate the Need and Confirm the Source.
Technology has changed, and so have its attackers.

Today's attacks are more advanced and believable than ever.

Use Caution With Unexpected Links and Attachments.

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
Look after your keys.

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
This is a key.

This is a key.

This is a key.

Treat all your keys with care.
Your Dog’s Name Is Not a Password

Choose a password that is easy to remember, yet hard to guess.

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

Never click on unexpected email links or attachments.
Patrol Your Security Perimeters

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

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00098-01 • 20110318
What’s In Your Computer?

Scan Regularly for Viruses

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

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00096-01 • 20110120
What’s In Your Computer?

Scan Regularly for Viruses
Only share company information with those who need to know.

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
Only share company information with those who need to know.

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

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00091-01 • 20110120
Only share company information with those who need to know.
Don’t Get Hooked

Beware of phishing scams.

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

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00089-01 • 20110120
Avoid Phishing Scams

Use caution with unexpected emails.
HOW WOULD YOU KNOW

IF YOUR CYBER ASSETS WERE BEING EXPLOR ED AND EXPLOITED?

ACCESS LOGS AND SYSLOGS

EVENT REPORTS

SEQUENTIAL EVENTS REPORTS

INFORMATION AT ADJACENT STATIONS

ALARMS

PRECISION TIMING

SYSTEM DESIGN CHOICES
HOW WOULD YOU KNOW

IF YOUR SYSTEMS WERE BEING EXPLORED AND EXPLOITED?

Read “How Would We Know?” at www.selinc.com/cybersecurity.

PRACTICE SECURITY IN DEPTH
Keep him out to keep the lights on.

Practice Security In Depth

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
The best cybersecurity has many layers.

Practice Security In Depth
The best security has many layers.

Practice Security In Depth
Don’t Use the Default Password
DON'T USE DEFAULT PASSWORDS
I DON'T SHARE MY TOOTHBRUSH OR MY PASSWORD!

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

© 2010 by Schweitzer Engineering Laboratories, Inc. • LM00074-01 • 20101026
DON'T
SHARE
YOUR
PASSWORD

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

© 2010 by Schweitzer Engineering Laboratories, Inc. • LM00073-01 • 20101026
USE SECURE BUSINESS PRACTICES

ONLY USE USB DRIVES YOU KNOW ARE CLEAN
KEEP YOUR TOOLS CLEAN

Always check for viruses before using USB sticks

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity
© 2010 by Schweitzer Engineering Laboratories, Inc. • LM00067-01 • 20101026