KEEP YOUR TOOLS CLEAN

Always check for viruses before using USB sticks
USE SECURE BUSINESS PRACTICES

ONLY USE USB DRIVES YOU KNOW ARE CLEAN
USE STRONG PASSWORDS

Weak: Webster

Strong: W3b$st3r

Stronger: A phras3 1s 3v3n Str0ng3r!
USE STRONG PASSWORDS

Weak: Webster
Strong: W3b$st3r
Stronger: A phras3 1s 3v3n Str0ng3r!
USE STRONG PASSWORDS

Weak: Webster
Strong: W3b$st3r
Stronger: A phras3 1s 3v3n Str0ng3r!
I Change My Password Regularly
DON'T SHARE YOUR PASSWORD
I DON'T SHARE MY TOOTHPASTE OR MY PASSWORD!
DON'T USE DEFAULT PASSWORDS
Don’t Use the Default Password
The best security has many layers.

Practice Security In Depth
The best cybersecurity has many layers.
Keep him out to keep the lights on.

Practice Security In Depth
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
HOW WOULD YOU KNOW

IF YOUR CYBERASSETS WERE BEING EXPLORED AND EXPLOITED?

ACCESS LOGS AND SYSLOGS
EVENT REPORTS
SEQUENTIAL EVENTS REPORTS
INFORMATION AT ADJACENT STATIONS
ALARMS
PRECISION TIMING
SYSTEM DESIGN CHOICES
Avoid Phishing Scams

Use caution with unexpected emails.
Don’t Get Hooked

Beware of phishing scams.

SCHWEITZER ENGINEERING LABORATORIES, INC.
Only share company information with those who need to know.
Only share company information with those who need to know.
Only share company information with those who need to know.
Only install SAFE SOFTWARE FROM LEGITIMATE SOURCES.
Is your software from an approved source?
What’s In Your Computer?

Scan Regularly for Viruses
What’s In Your Computer?

Scan Regularly for Viruses
 Patrol Your Security Perimeters
Myth #1  Viruses are just a nuisance.
Viruses and malware are serious problems that can do severe damage to your system. Take them seriously, and address infections immediately.

Myth #2  Isolated systems, such as substations, don’t need to run antivirus.
Many people assume that only systems with Internet connections need antivirus. All systems, isolated or not, should run antivirus or another type of compensating access control (e.g., whitelist).

Myth #3  You would know if you had a virus.
Many times, viruses go undetected by users for weeks, months, or even years. Scan your devices regularly.

Myth #4  Only Windows® gets viruses.
While Microsoft® Windows is highly targeted by attackers, other operating systems and devices are also susceptible to malware. Use caution and proper safeguards with all devices—from your smartphone to your Mac®.

Myth #5  As long as you have antivirus, your computer is safe.
Antivirus is a great tool, but it won’t protect you from all threats. Practice defense in depth, and layer your security.
Every Computer Deserves a Clean Environment!

Don’t pollute your computer with unnecessary applications and devices.

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.
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.

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00119-01 • 20111202
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.
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.

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00121-01 • 20111202
Security requires more than just fancy equipment.

Common Sense Is Your Most Valuable Tool

Analyze your surroundings.
Practice defense in depth.
Only share information on a need-to-know basis.
The More Variety, the Better!

Use Unique Passwords for Different Accounts

For information about SEL cybersecurity solutions or copies of this poster, visit www.selinc.com/cybersecurity.
Things Aren’t Always What They Seem

Phishing attacks have become increasingly sophisticated. Use common sense and care to separate legitimate from false claims.
Things Aren’t Always What They Seem

Phishing attacks have become increasingly sophisticated.

Use common sense and care to separate legitimate from false claims.
This is a key.

This is a key.

This is a key.

Treat all your keys with care.
Look after your keys.
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.

© 2011 by Schweitzer Engineering Laboratories, Inc. • LM00130-01 • 20111202
Technology has changed, and so have its attackers.

Today’s cybercriminals combine advanced technology with social tactics to steal information.

Validate the Need and Confirm the Source.
Yesterday’s Hacker

Today’s attackers are more advanced and malicious than ever.

Cybercrime is an international, multi-billion dollar business.

Be Aware. Be Ready.

Today’s Attackers
Today's attacks are more advanced and persistent than ever.

Always Investigate Unusual Behavior On Your System.