EVERYDAY SECURITY

INFORMATION SECURITY FOR YOUR BUSINESS

TIM PADGETT – TECHNOBILITY.US
THE SECURITY PROBLEM

Many problems, but some problems are more likely than others
RUSSIAN HACKERS? YOU BET… BUT THEY’RE NOT AFTER YOU.

SOPHISTICATED ATTACKERS

RUSSIANS HACKED

OPPORTUNISTS
YOU ARE THE TARGET OF OPPORTUNISTS, AND THEY’RE GETTING STRONGER

You, your employees, and your systems are the opportunity
DENY THE ATTACKER OPPORTUNITY AND/OR VALUE – Here’s how
YOUR EXPOSURE TO THE PROBLEM

You have a great degree of control over this— if you deny the opportunity to steal value
USING THE WEB

You can’t get from your business to your customer directly, you have to move through the net. This fact presents an opportunity – deny it. Can’t secure the nodes, but you CAN secure what passes through the lines.
USING THE WEB

Stay away from risky neighborhoods, stick with the well-known

Some neighborhoods are better than others, your browser can help
USING EMAIL

Email is NOT different from the web – same net structure applies, same problems

Every message passes through nodes you know nothing about, and a copy is made

Targeted communication is an opportunity to attack your systems and steal your information
ACCEPTING CREDIT CARDS

• Treat credit cards as if they are hand grenades – use them, and then get as far away as you can, as fast as you can. Fastest way to blow up your business.

• NEVER store them in any form or fashion, anywhere. Secure storage is beyond the capability of most small businesses

• Hidden access to a credit card is an opportunity to steal money

• Outsource this risk and cost to those that can handle it (PayPal, Square, etc.)
ANOTHER PERSPECTIVE

Information Assurance – Security, and more
INFORMATION ASSURANCE

- Larger than Information Security
- Emphasis on Preparation and Readiness
- Wider universe of threats – many of them are not attackers, but circumstances
- Lack of readiness is an **opportunity** to damage your **equipment** and cost **money**
  - Heard of Mr. Murphy?
INFORMATION ASSURANCE

• Don’t store anything you don’t have to store
  • Credit cards, inventory, cash
• Backup, backup, backup
• Data AND power
• Don’t keep your backups in the primary location
  • Online backups (IDrive, Backblaze, etc.) – benefits and limitations
GREAT. NOW WHAT?

You can do a lot for a little
OK – WHAT’S THIS GONNA COST ME?

- Cost directly related to the number of *opportunities* you present and the *value* of what you protect
- Learning is cost-effective, and *being smart is free*
- The smart thing to do is make sure what YOU care about is protected
  - Do you care if someone uses your WiFi for free?
- Your legal duty is to take “reasonable and customary” measures
- Trade-off: Cost to secure vs. impact of a breach
FREE STUFF TO DO

BEING SMART IS FREE

• Two-factor Authentication (TFA) – Bad Guy has to have your password AND your phone

• Use a password manager (LastPass, etc.)
  • Generate and keep random passwords and other information there

• Hide your WiFi

• Don’t use your business/public email address as a username anywhere

• Don’t answer security questions honestly
  • “What’s your mother’s maiden name?” – SmithGNXLUB
FREE STUFF TO DO

- **Use**: Use the “plus sign” feature in Gmail
- **Avoid**: Avoid open networks (Starbucks, Sam’s, etc.) unless you use a VPN
- **Work**: Work with companies that have outside auditors
- **Check**: Check your insurance for cyber specifics
- **Make**: Make a plan for a cyber theft response
- **Make**: Make a plan for disaster recovery
- **Learn**: Learn, learn, learn
USEFUL PLACES AND THINGS

• Hotspot Shield VPN  https://www.hotspotshield.com/
• LastPass Password Manager  https://www.lastpass.com/
• HubSpot CRM  https://www.hubspot.com/products/crm
• PCI Self-Assessment Questionnaires (SAQs)  https://www.pcisecuritystandards.org/document_library?category=saqs#results
USEFUL PLACES AND THINGS

• Stay Safe Online (National Cyber Security Alliance)
  https://staysafeonline.org/cybersecure-business/

• Testimony before the Small Business Committee, Howard S. Marshall, FBI Deputy Director

• Stop/Think/Connect – Homeland Security/FBI/NSA effort
  https://www.stopthinkconnect.org/

• Payment Card Security Standards https://www.pcisecuritystandards.org/
ABOUT TIM AND TECHNOBILITY

• 25 years experience in IT
• Master of Science, Information Technology (focus on Information Assurance)
• MBA, Information Technology
• Certified Project Management Professional (PMP)
• Technobility’s Goal – making technology useful by making it understandable
• tim@Technobility.us
• www.Technobility.us