Cybersecurity 103A:
Wolves in Sheep's Clothing &
How to Keep from Being Sheared

Officially Abridged Edition

Blue Valley Technologies
& Networks Plus

What is the biggest security risk facing your business?

Nope…

Human Error!

According to NIST, over 90% of cyber-incidents are directly attributable to human error

Thoughts on Cybersecurity

- **Cybersecurity is _not_ simply a technology problem, it is a new thought process and approach.**

- "If you think technology [alone] can solve your security problems, then you don't understand the problems and you don't understand the technology." – _Bruce Schneier_
- "There are risks and costs to a program of action—but they are far less than the long range cost of comfortable inaction." – _John F. Kennedy_

Scary Statistics!

- McAfee Labs recorded an **average** of 5 new malware samples per **second!**
  (McAfee Labs Threat Report, June 2018)

- Of companies that suffer catastrophic data loss:
  - 43% never reopen
  - 51% close within two years

- Ransomware caused $325 million in damages in 2015, over $5 billion in 2017, and is expected to exceed $11.5 billion annually in 2019!
  (Cybersecurity Ventures, 2017)
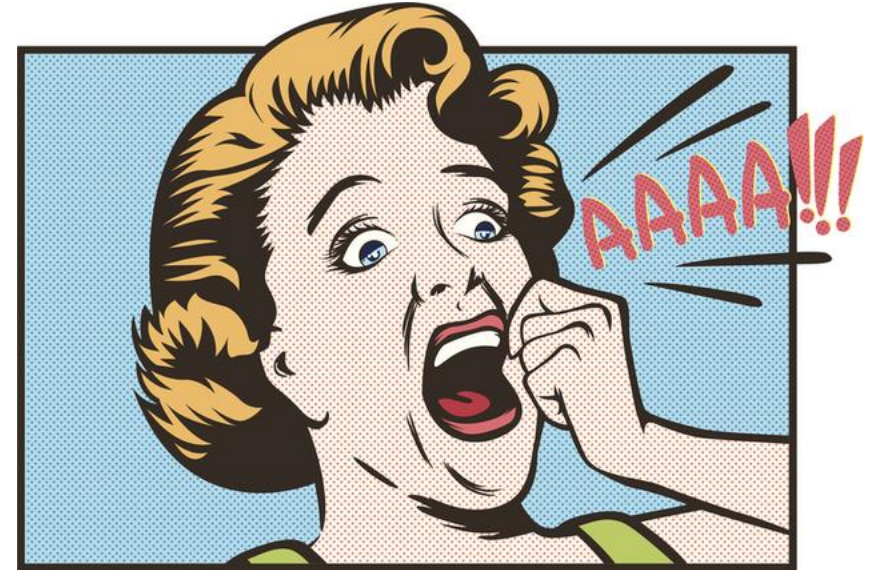
Cybersecurity – How to be a Sheep in Wolves' Clothing
The Road to Cybersecurity

Most of these are easy and fairly inexpensive to implement.

Patches & updates

Identity management and MFA

Security software/hardware

Reliable backups

What's your biggest security risk?

The person looking back at you in the mirror.

STOP. LOOK. THINK.
Don't trust anything.
Verify everything.

Gone Phishing

Social Engineering via phishing or vishing is clearly the biggest threat!

- **So, how do you recognize it?**
  - **Who sent it?**
    - **But I know this person! –** Maybe not. Double-check!
  - **Who was it sent to?**
  - **When was it sent?**
  - **What is it about?**
    - Does it request urgent action?
    - **P.S. –** Bill Gates is not going to send you money, Microsoft doesn't track your emails, and no Nigerian Prince is really going to send you a million dollars…
  - **Is there an attachment or link?**

WHO IN YOUR ORGANIZATION IS GOING TO TAKE THE HACKER'S BAIT?

Free WiFi? Isn't that cool!

Uhhh…no…
Here are some tips for mobile security:
- Don't use 'free' Wifi
  - Use a VPN If you have to use WiFi in a public area
- Turn off your Bluetooth when you don't need it!
- Use Multifactor Authentication whenever it is possible
- Use encryption whenever you can!

What Else Can I Do to Protect Myself?

- **Defense in Depth – A Primer**
https://networksplus.com/resources/blogs

- **Go back to rules 1 and 2: STOP. LOOK (or LISTEN). THINK. DON'T TRUST ANYTHING. VERIFY EVERYTHING.**

- Remember that old adage: IF IT SOUNDS (OR LOOKS) TO GOOD TO BE TRUE, IT PROBABLY **ISN'T...**

- Finally...Learn as much as you can about the current threats. Knowledge is power, especially with security!

Practice these rules every time, no matter where you are!

NETWORKS PLUS | bluevalley TECHNOLOGIES

800.299.1704 | networksplus.com
Locations in Home | Manhattan | Topeka | Salina

JERRY HORTON, IT DIRECTOR
jhorton@networksplus.com

QUESTIONS?