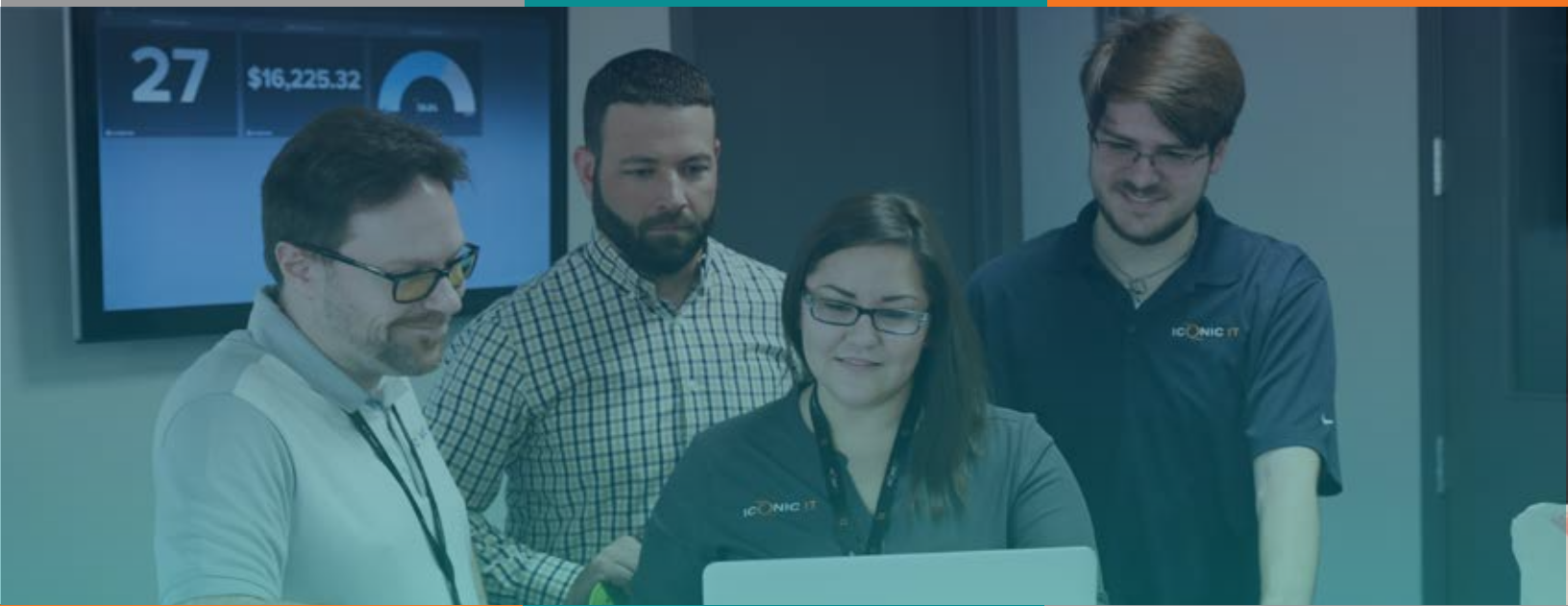
ICONIC *Education*
Powering businesses through education.

PRESENTATION OUTLINE

SMALL BUSINESS SECURITY ESSENTIALS

ICONIC IT
better together



INTRO

It's easy for users to be overwhelmed with all the information available on cybersecurity and network safety. There must be balance between security and functionality for users. Too much information, and they may be tempted to "tune out." Too little, and they may not be prepared for potential cyber attacks. The best approach is giving your employees exactly what they need to play their part in keeping your network secure.

TODAY'S THREAT LANDSCAPE

PHISHING

General Phishing

Sending out emails requesting personal information to a large amount of email addresses. This casts a wide, generic net to capture as many victims as possible.

Spear Phishing

A more targeted approach to phishing. This method finds personal information about employees and uses it as a tool to find out sensitive data about them.

Social Engineering / Spoofing

Hackers pose as another source known to the victim to gather information. Email is just one approach to spoofing. Hackers can replicate websites to near perfection; the user will be unaware that he or she is on a phony website and will give financial data, passwords, and other sensitive data.

Phishing Prevention and Tools

- Internal codes for transactions / Dual approval
- Email Filtering
- REPEL Method

R	**Requested:** What did the email request? Would you expect the sender to need the information requested?
E	**Email Address:** Look at the address. Is it legitimate? Look for common spoofing clues, like changing a domain from ".com" to ".net."
P	**Personal Information:** Is the email requesting personal information? If so, are they requesting it via a clickable link?
E	**Errors:** Are there errors in grammar, spelling or context? Is the company name misspelled in the email address?
L	**Links:** Hover over links to see where they actually point. Do not click any link that doesn't come from a valid source.

Real World Discussion

The recent election hacking was done through spear phishing methods.

HACKING

Brute Force Attack

A brute force attack attempts to crack passwords by trying every possible password combination. This method takes a while, since computer programs need to guess the passwords.

Dictionary Attack

This form of attack works by guessing your password by using actual words, or those found in the dictionary, combined with commonly used characters. This is why security experts always recommend using nonsensical, or non-dictionary words.

Compromised Database

When large website databases containing usernames and passwords are stolen, bad actors distribute them on the internet. This is why it is a bad idea to reuse usernames and passwords.

Vulnerability /Zero day / Exploitation

Software is "patched," or updated with fixes for flaws in security and functionality, continuously. Sometimes, hackers find these gaps in security before developers have the opportunity to patch them.

What you or your company could be held responsible for:

- HIPAA violations
- Financial Data
- Client data/ law/ sensitive info
- Overview of penalties

Hacking Prevention and Tools

- Password management and two factor authentication
- Password length and complexity
- Layered Security
- Changing default passwords
- Access Control
- Physical Security

RANSOMWARE

What it Does

- Holds data for ransom
  - Can delete files
  - Encrypts files
    - –May or may not be able to be unencrypted

How Do You Get Ransomware

- Email
- Drive-by downloads
- Public facing access to network with weak account passwords
  - Example: A client's scanner's password was 'scanner." A hacker easily figured this out and put ransomware on their network.

How to Prevent and Recover from Ransomware

- Backups
  - If you are infected with ransomware, having backups in place means you can easily restore your data.
- Do not pay ransoms.
  - The FBI reports that companies are often not given decryption keys after paying the ransom.
  - Absolute last resort, and only after authorities have exhausted all other avenues
- Strong passwords on networks
- Anti-virus that can detect ransomware
- Layered security
- Policies against zip files
- Care with PDF's
  - Malware masked as Word Documents and PDF's

WRAP UP

- Pay attention/ be vigilant
- When in doubt, turn the computer off and call IT support
  - If the computer is not on, files cannot be encrypted and the virus will be isolated to the affected machine.
- Always verify with people if something seems strange. If something is truly legitimate and urgent, they will resend the message or verify that they sent it. When in doubt, don't click the links in your emails or attachments, and never give information via a clickable link.