Cybersecurity Basics for Small Businesses

Michelle Reinen – Division of Trade and Consumer Protection

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

CYBERSECURITY

- Cybersecurity Basics
- Physical Security
- Vendor Security
- Threats
- Next Steps
- Resources

WHAT CYBER CRIMINALS WANT

Personally Identifiable & Sensitive Business Information

- TIN Number
- EIN Number
- Registered Agents
- SS# / DOB
- Business Credit Cards
- Proprietary Business Info
- Email Addresses
- Passwords
- Financial Account Numbers
- 3rd Party Vendor Info
- Phone Numbers
- Customer/Employee Info

LEADING CAUSES

- POS Intrusions
- Web app attacks
- Insider Misuse
- Physical Theft/Loss
- Crime ware
- Card Skimmers
- Cyber espionage
- Misc. Errors

EMPLOYEE RISK FACTORS

- Browsing Habits
- Email Attachments
- Spam
- Backups
- Unauthorized Software
- USB Drives
- Social Media
- Mobile Devices
- Not Shredding

CYBERSECURITY BASICS

Video: Cybersecurity Basics | Federal Trade Commission (ftc.gov)

CYBERSECURITY BASICS

- Protect Files & Devices
  - Update Software
  - Secure Files
  - Back-up Files
  - Require Passwords
  - Encrypt Devices
  - Use Multi-factor Authentication (MFA)
- Protect Your Wireless Network
  - Secure your Router
  - WPA2 Encryption
  - Use MFA
  - Require Complex Passwords & Change Them
- Train All Staff
- Have a Plan

PHYSICAL SECURITY

- Protect Equipment and Paper Files
  - Store Securely
  - Limit Access
  - Send Reminders
  - Keep Stock
- Protect Data on Your Devices
  - Limit Log-in Attempts
  - Encrypt
  - Use MFA
  - Require Complex Passwords

VENDOR SECURITY

- Monitor Vendors
  - Put it in Writing
  - Verify Compliance
  - Make Changes as Needed
- Safeguard Your Business
  - Control Access
  - Secure Your Network
  - Use MFA

THREATS & SCAMS

- Tech Support
- Phishing & Fake Billing
- Ransomware
- Business Email Imposters

TECH SUPPORT SCAMS

- Phone Call, Pop-Up or Email
- Problem with your Computer
- Money, Personal Information, Access to Files
- Harm your Network, Data at Risk, Damage your Business
- Hang-Up / Ignore It
- If worried – Call Your Security Software Company.

PHISHING & FAKE BILLING

- An email – that LOOKS like it is from someone you know – one of your company's vendors.
- Click a link to update your business account.
- It looks REAL.
- It looks urgent – ACT NOW – or something bad will happen.
- If you click…
  - Install ransomware
  - Access to accounts
- Check It Out!

RANSOMWARE

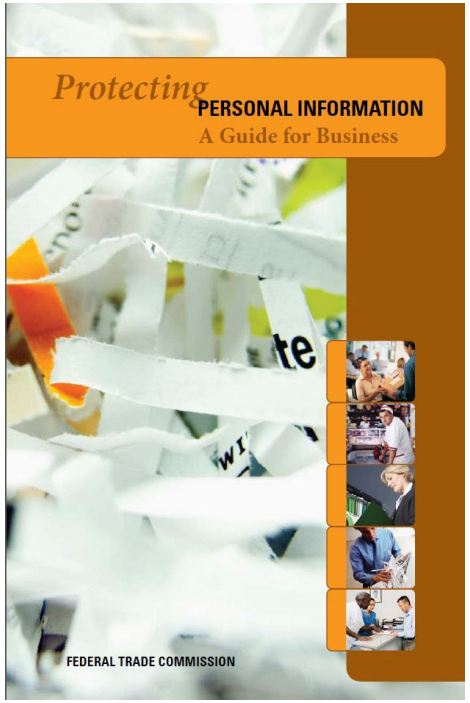
- Security
- Training
- Most Vulnerable
  - Bad password practices
  - Leave remote-access ports open to the Internet unprotected
  - Networks that don't patch quickly

BUSINESS EMAIL IMPOSTERS

- Email looks like it is from your Company (Spoofing)
- Employee Payroll or Impersonate a Customer/Vendor
- Best defense = Process
- ANY request to change a bank account MUST be authenticated to the requestor through a TRUSTED channel.

NEXT STEPS – MINIMIZE THE RISK

- Protect Personal information
  - Take Stock
  - Scale Down
  - Lock It
  - Pitch It
  - Plan Ahead
- Evaluate your Options
- Train Employees
- Recognize the Warning Signs



EVALUATE YOUR OPTIONS

- Email Authentication
- Cyber Insurance
- Hire a Web Host
- Secure Remote Access
- Policy & Procedures
- Training Plans

Implement Changes!

TRAIN EMPLOYEES

- Cyber Security Practices / Procedures
  - Shred documents
  - Erase data correctly
- Response Plan
- Reporting
- Scams / Threats
- Warning Signs

RECOGNIZE THE WARNING SIGNS

- Unauthorized debit and credit charges
- Business email compromise attempts
- Unsolicited change of registered agents
- Business computers and phones are infected with ransomware/malware
- Fraudulent business loan applications
- Bill collectors are calling
- Denied credit

RESOURCES

Federal Trade Commission - FTC Cybersecurity for Small Business

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

Federal Communications Commission - 10 Cyber Security Tips for Small Business

https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

NIST Small Business Cybersecurity Corner

Small Business Cybersecurity Corner | NIST

National Cyber Security Alliance (NCSA) Small & Medium Sized Business Resources

CyberSecure My Business™ - National Cybersecurity Alliance (staysafeonline.org)

Additional Resources

Check out these additional resources like downloadable guides to test your cybersecurity know-how.

Guide for Employers

Start a Discussion

Cybersecurity Quizzes

Test Your Knowledge

Get the Materials

Download Materials

Order Free Publications

Cybersecurity Video Series

See All Topics

More FTC Small Business

Go to FTC.gov/SmallBusiness

Sign up to Receive the FTC Business Blog

Sign Up

RESOURCES

Linked In

Facebook

Instagram

Twitter

Consumer Protection

REQUEST A PRESENTATION

@ DATCP.WI.GOV

1-800-422-7128

- General Consumer Protection
- Cybersecurity Basics for Business
- Common Scams & Fraud
- Identity Theft & Privacy Protection
- Scams & Fraud Targeting Small Businesses
- Privacy & Security for Businesses

RESOURCES – CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY (CISA)

CISA.gov/news-events/cybersecurity-advisories – Includes alerts and advisories (including former US-CERT information)

CISA.gov/known-exploited-vulnerabilities-catalog – Known Exploited Vulnerabilities (KEV) catalog

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report:

CISA.gov/report
24x7 contact number: 888-282-0870
Email: Report@cisa.gov

CISA field personnel in Wisconsin:

Dan Honore, Cybersecurity Advisor, daniel.honore@cisa.dhs.gov

Bill Nash, Cybersecurity Advisor, william.nash@cisa.dhs.gov

John Busch, Protective Security Advisor, john.busch@hq.dhs.gov

David Melby, Protective Security Advisor, david.melby@cisa.dhs.gov

RESOURCES

GOVERNOR'S CYBERSECURITY SUMMIT 2023

2023 WI Cybersecurity Summit (eventsair.com)

WEM.WI.GOV

1-800-422-7128

DATCP.WI.GOV

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION (DATCP)

October 2023