



Cyber security is profoundly important. Cyber crime affects all industries and criminals disproportionately target SMBs. The Ponemon Institute reported in November 2018 that nearly 70% of cyber attack victims were SMBs with fewer than 250 employees.

Data breach, ransomware, and similar cyber attacks can cause excessive costs in regulator fines, breach mitigation, and even lawsuits. Most business don't recover from cyber attack, costing jobs and financial security.

We at SynchroNet work hard behind the scenes to protect your data and productivity, but we are partners in the fight against bad guys. Stop, look, and think before you click. Our process + your vigilance means we can successfully thwart the bad guys.

The SynchroNet Cyber Way

Better cyber security begins with The SynchroNet Way and ends with you.

Financial Impact of Cyber Crime

\$1.9 Million

Average cost of a "small" security breach. Costs of more typical breaches with 50,000+ records exceed \$7M and rise to hundreds of millions of dollars.

\$160/Record

Average cost per compromised record of PII (personally identifiable information)*. Breach costs include cyber security consultants, regulatory fines, lawsuits, and more.

*2018, Ponemon Institute/IBM Security

Common Types of Protected Information

Full Name	Social Security Number	Mailing Address	Zip Code
Credit Card Number	Email Address	Phone Number	Password
Driver's License Number	Date of Birth	Passport Number	Race
Bank Account Number	Mother's Maiden Name	Username	Gender

This is not an exhaustive list of all types of protected and related information that cyber criminals seek. Everytime you email protected information that includes sensitive information like this, you should use encryption, which is available through your email application. But first, think through how, why, and with whom you are sharing data.

Personal Impact of Data Breach



Lost Time



Lost Peace of Mind



Lost Trust



Job Insecurity

“95% of security breaches in 2018 were avoidable”

July 9, 2019, Internet Society (ISOC), a not-for-profit American watchdog organization

Your Vigilance

Your role in The SynchroNet Cyber Way includes doing your best to:

Avoid Business Email Compromise and Social Exploits

Minimize Accidental Disclosures of Information

Server-Level Malicious Email Blocking

Our Process

These critical tasks are already part of The SynchroNet Way.

The SynchroNet Cyber Way

Regular Risk Assessments

Promptly Patching Known/ Public Vulnerabilities

Properly Configured Devices and Services

Encrypted and Protected Data and Email

No End-of-Life/Unsupported Devices, Operating Systems, or Applications

Minimize Accidental Disclosures of Information

- 

Posted Data
- 

Security Policies
- 

Secure Access
- 

Zero Trust

Eliminate or lock away any sensitive data on or around your work area such as sticky notes with access points or passwords, etc.

Know the security policies that affect the data you work with every day like HIPAA or PCI DSS to be more alert to how you work with that data.

Limit or eliminate how much data you access outside of the network. Skip thumb/flash drives. Take advantage of Remote Access to ensure a secure connection.

Follow a Zero Trust policy. Verify requests for information, especially from people outside of your organization. Avoid sharing ‘the scoop.’ Don’t talk about secure data.

Password Security

Did you know that the two most common passwords in the English-speaking world are ... *Password* and *123456*?


1. When you’re asked to change your password, do so without delay
2. Pick combinations of simple words that you can easily remember. Inject numbers and special characters to create strong passwords, like *R3dFoxM@sk* or *sunny4Me*
3. If you’re worried about remembering so many passwords, set up a secure password vault like Keeper Vault, RoboForm, or a similar vetted utility

Don't Fall for the Bait of a Phishing Email

Practice Zero Trust (as in, verify everything!) when checking your email on both desktop and mobile devices. Always **Stop, Look, and Think** before taking action.


Email is the preferred attack vector for cyber criminals and is often ground zero for ransomware, viruses, malware, and more.

Follow these four strategies to see if an attachment or link is safe to open or click:




Email is Expected

If an email with an attachment is unexpected, call and confirm.




Name and Email Match

The sender's name should be reflected in the email address.



Accurate Links Upon Hover

Look out for URL mismatch, like *help.amex.com* vs. *amex.com*.

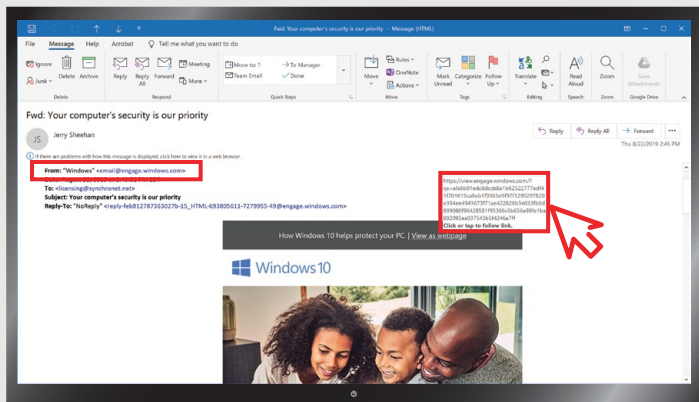


Brand and Product Match

Double-check branding to determine the actual sender.

Network Safety Starts with Email Safety

- ▶ Is this email **expected**? If not, call the sender, verify the email, and then move forward.
- ▶ Does the **name/email match**? Not sure? Call the sender for verification or skip the email.
- ▶ When you hover your mouse pointer over a link, do you see the **correct URL**? Or is there another domain before that first critical period, like *engage.windows.com* vs. *microsoft.com*?
- ▶ Is there a **brand/vendor mismatch**? Does the email come from the 'product' or from the 'company'?
- ▶ Is there **unusual urgency** in the message? If so, call the sender to verify the request or delete the email.
- ▶ Is the email requesting **confidential data** the sender should already have? Call to verify the request.
- ▶ Is the request in an **unusual format**, like a text message, asking you to update an app that you would normally update through the app store?




Call **Verify** **Move Forward**



If you click a link or open an attachment and an installation process initiates, do not 'wait and see'. Take immediate action! Unplug your device and call SynchroNet at 716-677-2677.