Cyber Crime Landscape

Why would a cybercriminal target your business?

You have what they want.

- Intellectual property
- Customer information
- Employee information (e.g. W2s, PII)
- Medical records

$2.1 trillion: The total global annual cost of all data breaches by 2019, as suggested by Juniper Research.

Because of the growth in data breaches, personal data is easier to buy on the dark web than ever. RSA reports personal data can cost as little as $0.20 to $15 USD.

Sources:
https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
https://www.rsa.com/content/dam/en/white-paper/2018-current-state-of-cybercrime.pdf

Who can expose your business?

Internal Threats

Employees

Vendors

- **Malicious:**
  stealing information
  (e.g., stealing customers information, card skimming)

- **Negligence:**
  lost resources storing information
  (e.g., laptops, smartphones, tablets)

External Threats

Individual threat actors

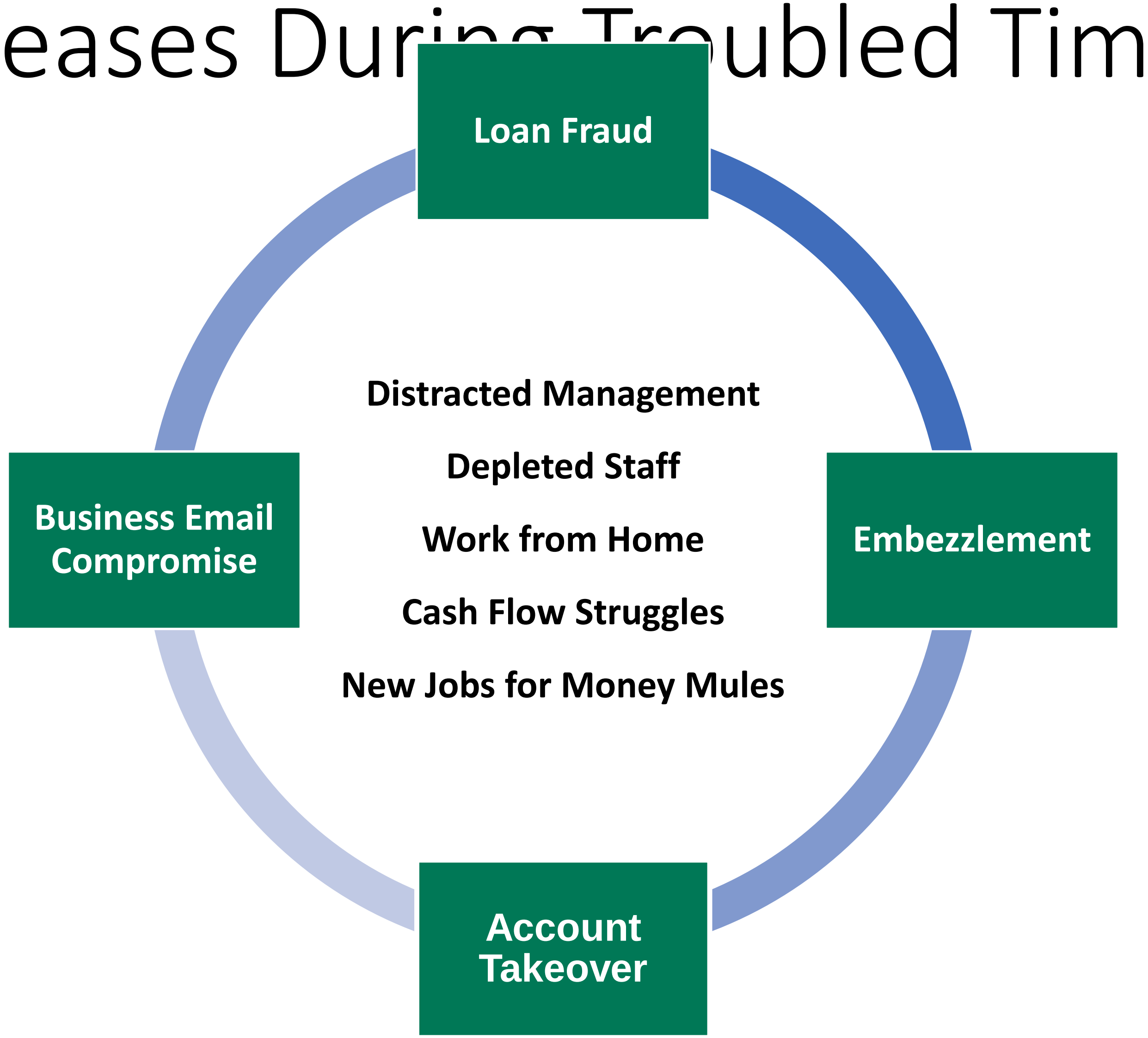
Hacktivists

Organized criminals

Nation-state

- Steal information
- Utilize viruses or malicious code
- Disrupt businesses via cyber vandalism
- Pursuing social or political agenda

Fraud Increases During Troubled Times



Loan Fraud

Embezzlement

Account Takeover

Business Email Compromise

Distracted Management

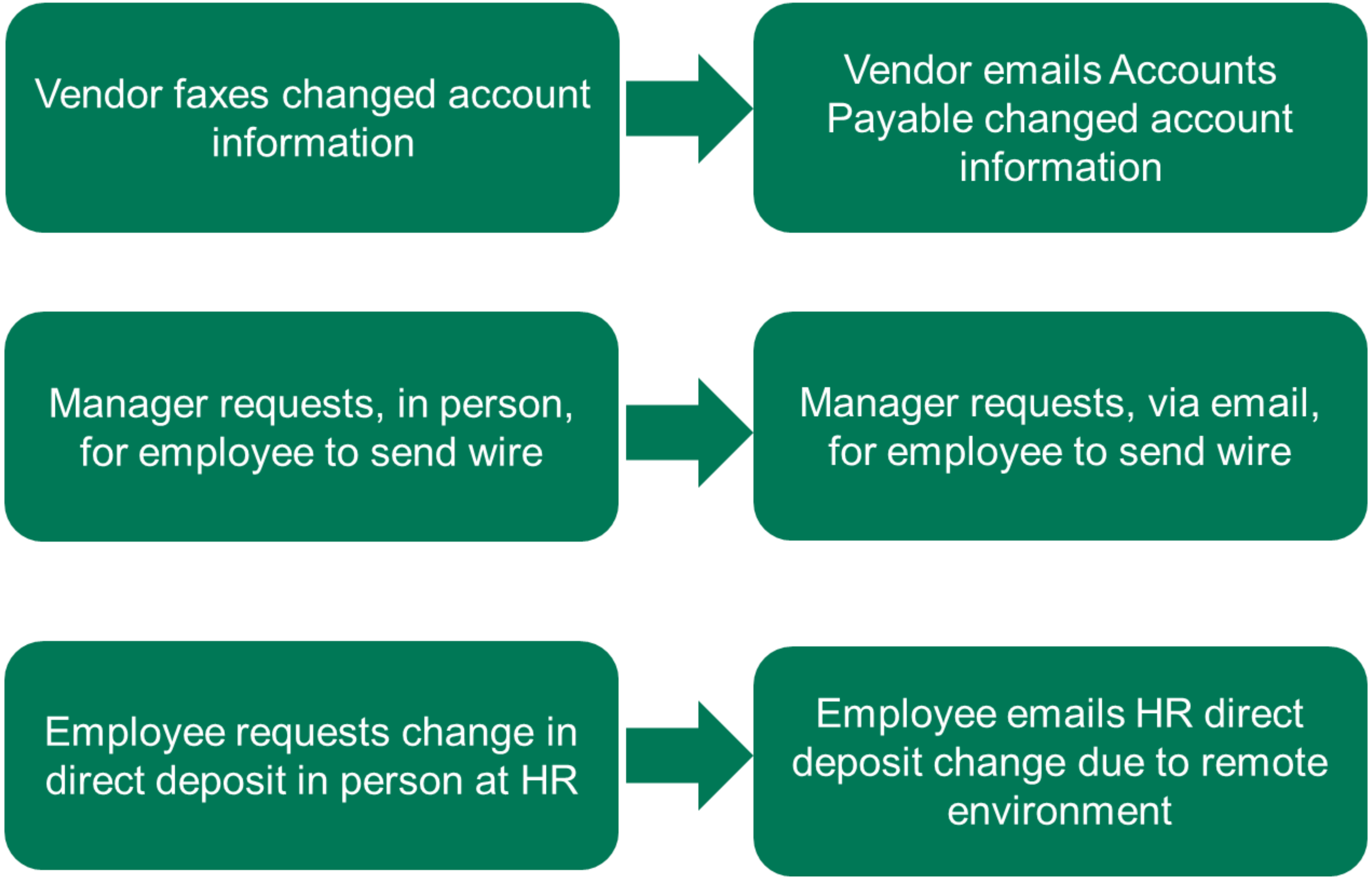
Depleted Staff

Work from Home

Cash Flow Struggles

New Jobs for Money Mules

What has changed with switching to a remote environment?



Vendor faxes changed account information → Vendor emails Accounts Payable changed account information

Manager requests, in person, for employee to send wire → Manager requests, via email, for employee to send wire

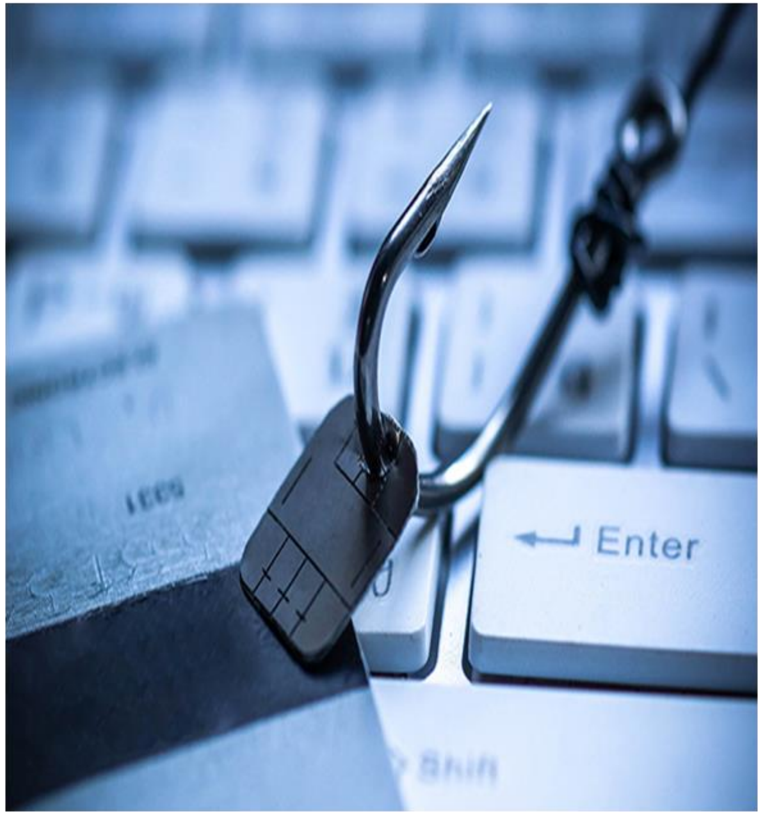
Employee requests change in direct deposit in person at HR → Employee emails HR direct deposit change due to remote environment

Phishing Attacks

91% of cyber attacks started as a phishing email

Phishing attacks **PREY** on curiosity, greed, great deals and emotion

A successful phishing attempt could **STEAL** your credentials, passcodes and place malware on your computer



Cyber Security Hygiene Tips: Phishing

1. Be wary of links or attachments. Hover over embedded links to reveal their destination

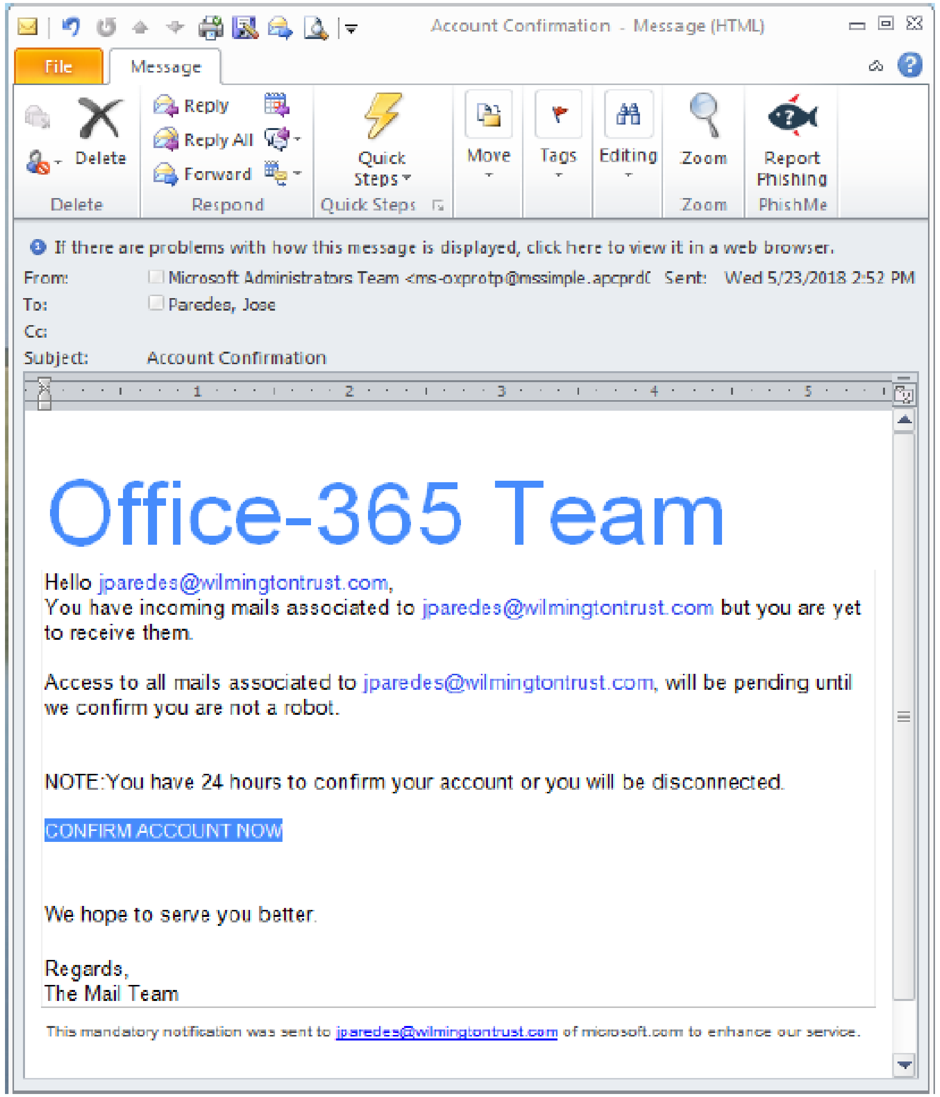
2. If in doubt of the legitimacy of an email, text or call, contact that person/ company using an authenticated source

3. Avoid using same password across different sites

4. Avoid using public Wi-Fi

5. If you receive a suspicious email that appears to be from M&T, forward it to phishing@mtb.com

Example Phishing E-mail reported by an M&T Employee



If there are problems with how this message is displayed, click here to view it in a web browser.

From: Microsoft Administrators Team <ms-oxprotp@mssimple.apcprd(Sent: Wed 5/23/2018 2:52 PM
To: Paredes, Jose
Cc:
Subject: Account Confirmation

Office-365 Team

Hello jparedes@wilmingtontrust.com,
You have incoming mails associated to jparedes@wilmingtontrust.com but you are yet to receive them.

Access to all mails associated to jparedes@wilmingtontrust.com, will be pending until we confirm you are not a robot.

NOTE:You have 24 hours to confirm your account or you will be disconnected.

CONFIRM ACCOUNT NOW

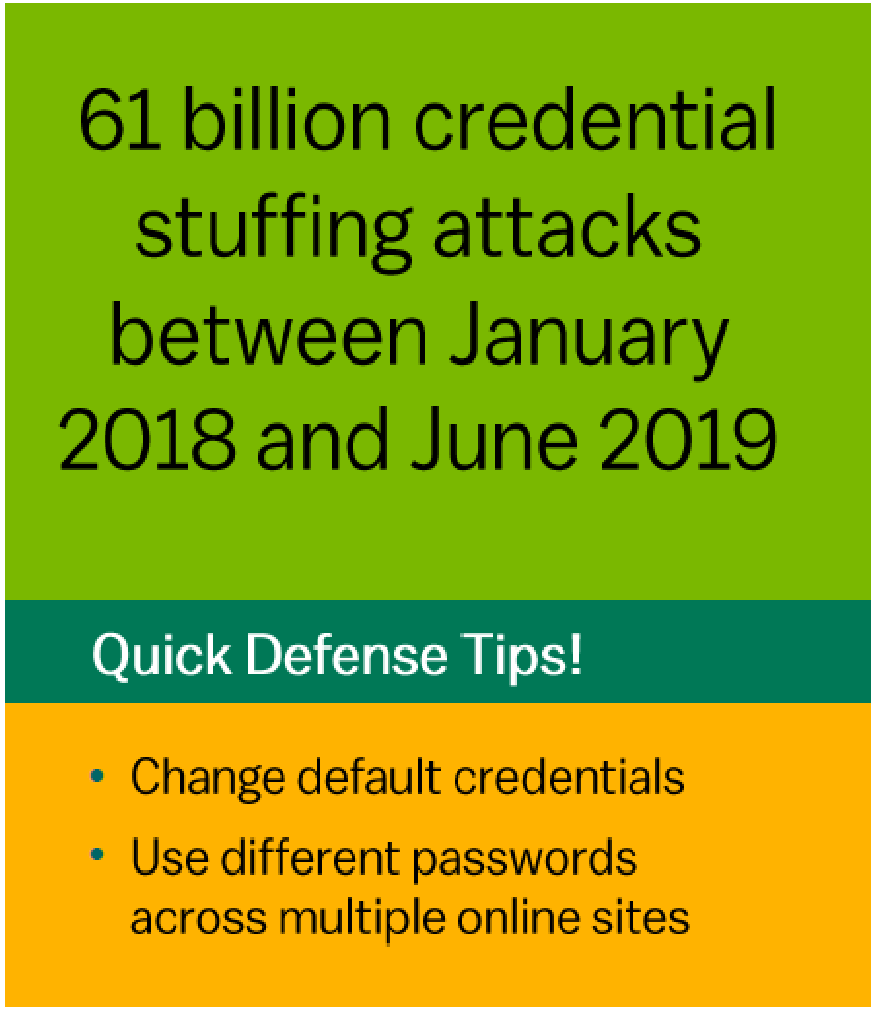
We hope to serve you better.

Regards,
The Mail Team

This mandatory notification was sent to jparedes@wilmingtontrust.com of microsoft.com to enhance our service.

Trends: Credential Re-use

Definition: An unfortunate trend where people re-use the same username and password on multiple sites



61 billion credential stuffing attacks between January 2018 and June 2019

Quick Defense Tips!

- Change default credentials
- Use different passwords across multiple online sites

Source: *blog.knowbe4.com/18-months-61-billion-credential-stuffing-attacks*

Cyber Security Hygiene Tips: Mobile Phones

1. Install anti-virus software on your phone
2. Subscribe to your mobile carrier’s anti-spam services
3. Utilize two-factor authentication when available
4. Enable remote tracking in case your phone is lost
5. Avoid using public Wi-Fi
6. Only download apps from your phone’s official app store
7. Configure auto-lock
8. Use a mobile VPN app
9. Don’t answer calls from numbers you don’t recognize
10. Check your phone settings for built-in call blocking
11. Disable the microphone on apps not needed
12. Keep your phone’s operating systems and apps updated

Cyber Security Hygiene Tips: Voice Assistants

- Microphones contained within smart speakers and mobile phones (for some apps) are configured to always be listening when they are powered on

- Third party employees may have access to voice recordings on Smart Devices

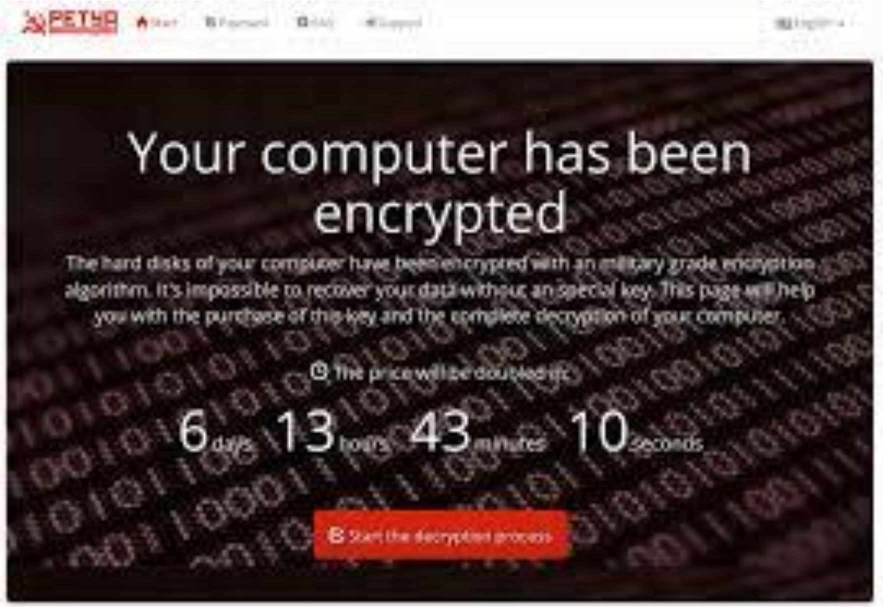
- Amazon Alexa, Google Assistant, iPhone and Android Phones all have settings to turn off microphones and/ or recordings

Ransomware

- A tactic involving the use of malicious software (malware) that, when downloaded to a computer, encrypts files so they can no longer be accessed – OR it locks down the operating system entirely so the user can no longer access anything.

- Typically delivered via email

- Ransomware damage costs will rise to $11.9 billion in 2019
  Source: KnowB4



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in

6 days 13 hours 43 minutes 10 seconds

Cyber Security Hygiene Tips: Ransomware

- Even when users recognize the tactics used by cybercriminals and adopt some security practices, ransomware may end up on the system even with the best precautions
- The FBI advises against paying the ransom because it doesn’t guarantee the information will be returned
- The best step against losing important files in a ransomware attack is to back up important files, so if they are encrypted, nothing is lost.

Quick Defense Tips!

- Update anti-virus software
- Be vigilant when opening emails
- Change default credentials

Source: 2017 Verizon Data Breach Report

Protecting yourself in a remote environment

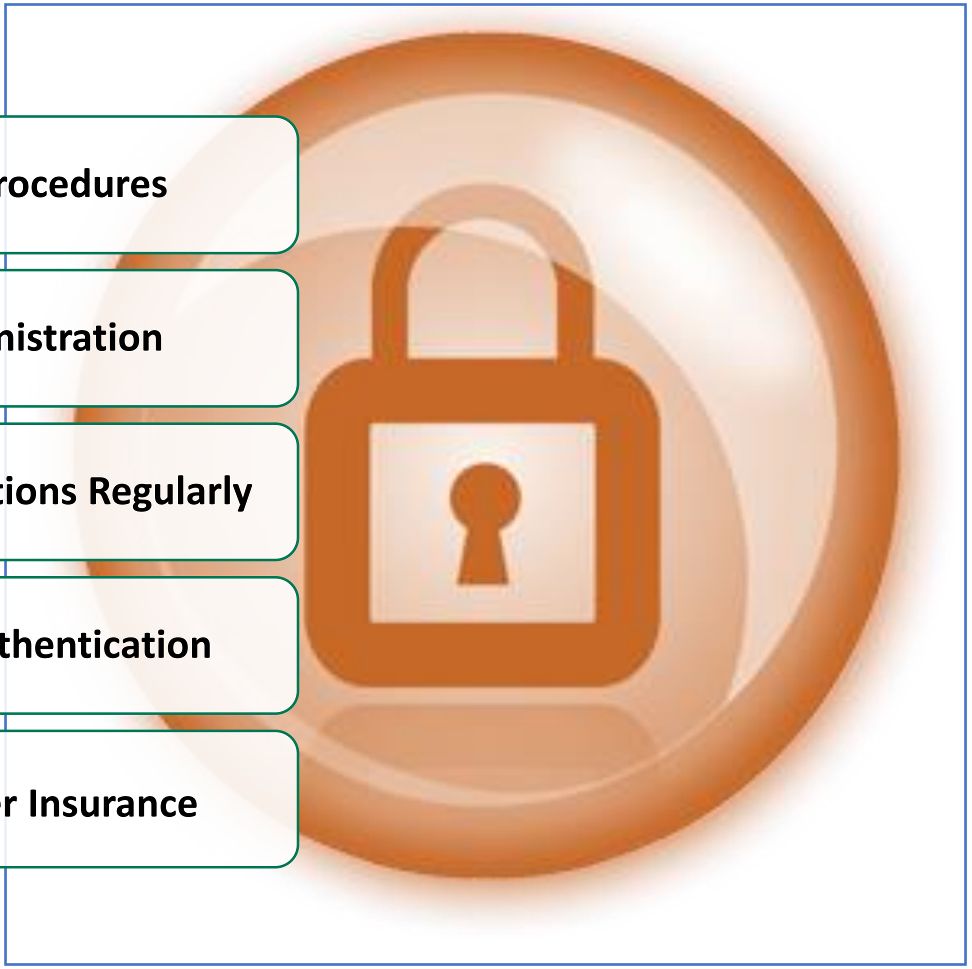
- Keep all networked devices updated
- Secure your router
- Use strong passwords and two factor authentication
- Keep regular backups

Securing Business Information

- Use corporate-issued devices for work only
- Stick with approved third-party services
- Password protected applications on mixed-use devices
- Shred physical documents

Photo source; sciencemag.com

Tips to Help Protect Yourself and Your Clients

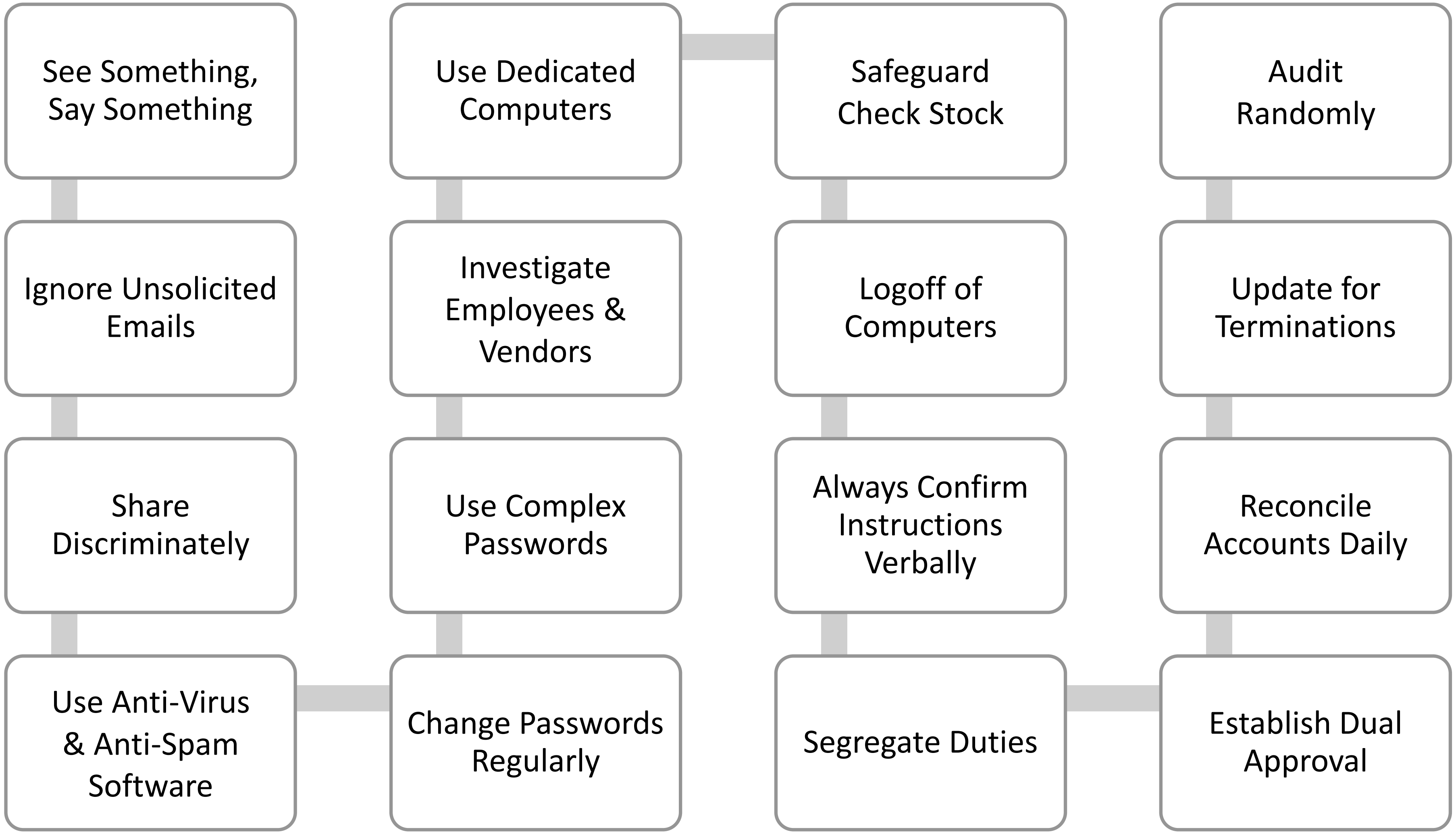


- Establish Procedures
- Dual Administration
- Review Transactions Regularly
- Two Layer Authentication
- Explore Cyber Insurance

Tips to Help to Protect Yourself and Your Clients

- Be Aware
- Verify Emails
- Run Up-to-date Endpoint Security Software
- Unique Passwords
- Fraud Prevention and Detection

Customer Controlled Best Practices



- See Something, Say Something
- Ignore Unsolicited Emails
- Share Discriminately
- Use Anti-Virus & Anti-Spam Software
- Change Passwords Regularly
- Use Complex Passwords
- Investigate Employees & Vendors
- Use Dedicated Computers
- Safeguard Check Stock
- Logoff of Computers
- Always Confirm Instructions Verbally
- Segregate Duties
- Establish Dual Approval
- Reconcile Accounts Daily
- Update for Terminations
- Audit Randomly