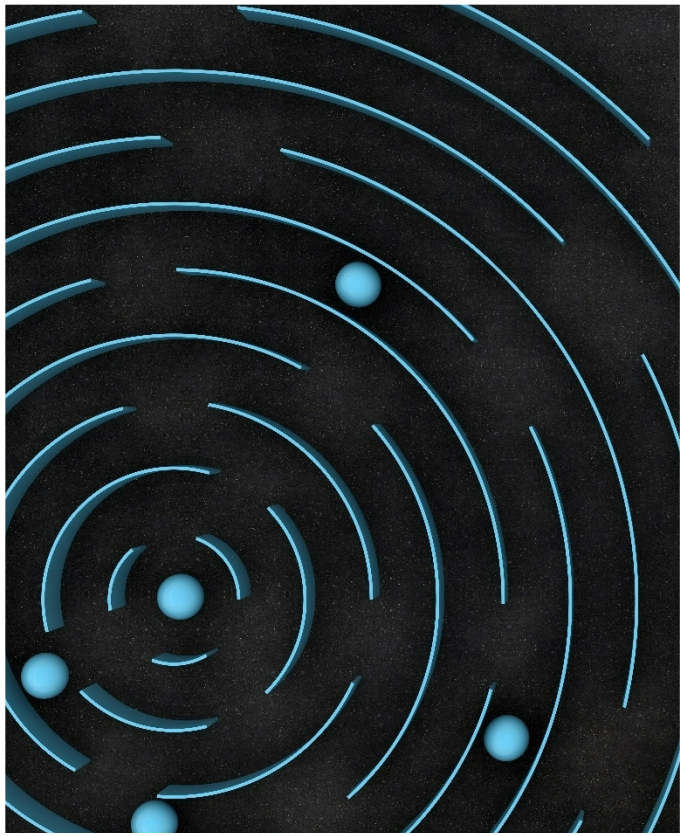
Cybersecurity Best Practices

Presented by

PPAI ONLINE™ Education



Presented By:

David Jackson, Sweda

Mike Pfeiffer, American Solutions for Business

Presenters

DAVID JACKSON
Director of Information Technology
Sweda Company

MIKE PFEIFFER
VP of Technology
American Solutions for Business

Mike Pfeiffer, VP of Technology
800.714.7298
mpfeiffer@americanbus.com
www.linkedin.com/in/mpcio

Cyber Safe Pledge™

American Solutions for Business strives to provide technology stewardship within the Print and Promotional Product industries. We value our partners and desire to conduct business safely and securely with each other.

These Top Ten focus areas are pragmatic Cybersecurity goals to pledge each other. At a minimum, the first point listed in each focus area should be accomplished as soon as possible.

Identity Management

Multi-Factor Authentication on systems that support MFA

Enforce Complex Passwords

SPF Records and DKIM signing for email

SPAM and Spoofing protection on email domains

Update & Security

Provide and require Security Awareness Training for Employees and Contractors

Antivirus and Malware protection on all systems. Definitions updated daily.

Apply High & Critical patches within 30 days of release to endpoints and servers

Policies & Planning

Disaster Recovery & Business Continuity written plan and tested at least annually

Security Incident / Data Breach Notification policy and process

Inventory of systems with access to business data

https://cybersafepledge.americanbus.com/

Cybersecurity Best Practices

- Develop Security Policies
- Device Management Policies
- Create an Incident Response Plan
- Security Awareness Training
- Multi-Factor Authentication (MFA)
- Anti-Virus & Anti-Malware
- Phishing Protection
- Data Backups

PPAI ONLINE™ Education

Develop Security Policies

- Create written policies
- Guidelines to inform staff on how to protect company data
- Define what security controls need to be established
- Example Policies
  - Password policies including strength & change frequency guidelines
  - Reporting lost or stolen devices
  - Company vs. personal equipment usage guidelines
  - Portable media policies (Ex: USB drives)
  - Security incident reporting
  - Data breach notification guidelines

Device Management Policies

- Company Issued vs. BYOD
  - Guidelines on what computers and devices can be used in your environment.
  - Access to systems is granted for non-sensitive systems & data
  - IT is allowed control over some aspects of the personal device
  - Create a corporate persona or container to restrict data storage
- Allowed Applications
  - Develop a list of Company Approved applications
- Updates
  - Create written policies to define frequency of patch deployment
  - High & Critical released patches to Servers within 30 days of release
  - Patch Management tools to Automate patching of applications
  - Develop guidelines for users to manually update other applications

Incident Response Planning

Steps to Take Before a Cyber Intrusion, Breach, or Attack Occurs:

1. Educate Sr. Management about Cyber Threats
2. Identify Critical Data or Intellectual Property
3. Have an Action Plan in Place Before an Intrusion Occurs
4. Engage with Law Enforcement Before an Incident
5. Ensure Organizational Policies Align with Your Cyber Incident Response Plan
6. Implement Appropriate Technology Before an Intrusion Occurs
7. Have Appropriate Authorization in Place to Monitor the Corporate Network
8. Ensure your Legal Counsel is Familiar with Incident Management to Reduce Response Time

Source: Department of Justice "Best Practices for Victim Response & Reporting of Cyber Incidents"

PPAI ONLINE™ Education

Security Awareness Training

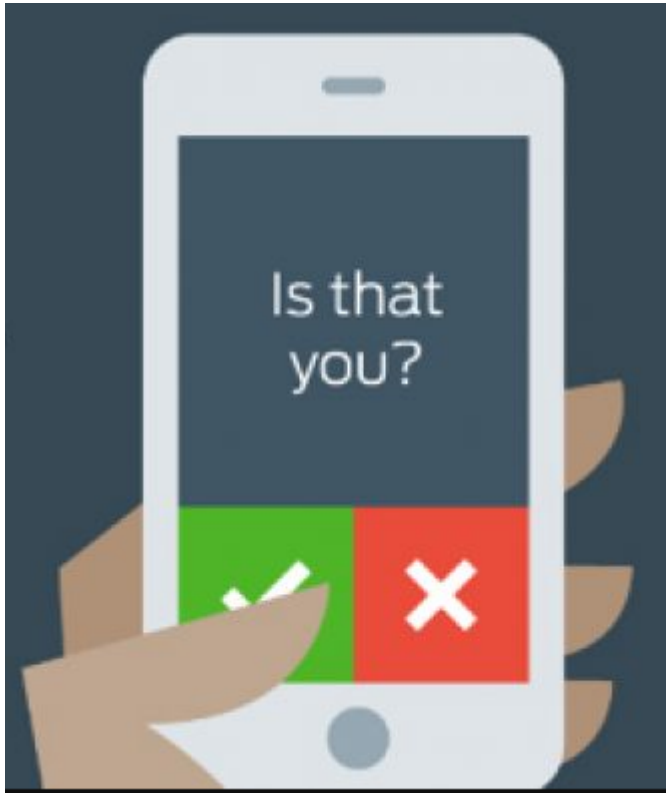
Mandate Full Participation – No Exceptions	Executives, Remote Workers, etc.
Baseline Assessments	Determine Existing Baseline Knowledge (Quiz)
Ongoing Assessments & Training	Training does not stick after one session
Reinforcement	Revisit key topics regularly to build a solid foundational knowledge
Tracking & Status Reporting	Develop Metrics to Track Success
Motivational Tools	Gamification

Source: The Center for Information Security Awareness

PPAI ONLINE™ Education

Multi-Factor Authentication (MFA)

- Sometimes referred to as Two-Factor Authentication (2FA)
- Implement MFA Across the Enterprise
- Passwords are no longer enough!
- Provide a Variety of Authentication Factors
  - Hardware Tokens
  - Soft Tokens
  - SMS/Text Messages
  - Phone Call
  - Email
  - Security Questions
- Do not put all your faith in MFA
- Do not make MFA Optional
- Do not only rely on Text Messages for the 2FA



Sources: ITPro Today and Centrify

PPAI ONLINE™ Education

Anti-Virus & Anti-Malware

- All Endpoints should be protected
- Frequent Signature Updates
- Define Exclusions
- First Defense for known Ransomware
- Protection of Sensitive Data
- Email Protection
- Ad-Blocking & Web Browsing Protection
- Don’t Forget Your Servers!

PPAI ONLINE™ Education

Phishing Protection

- 90% of all Cyber-attacks begin with a Phishing Email
- Company & Personal Reputation need to be Protected
- Mock Campaigns/Testing - To Trick or Not to Trick? That is the question!
- Training is Essential but not 100% Effective
- Train Employees to Trust but Verify
- Mitigation & Response is Continuous – No silver bullet solution
- MFA Significantly Reduces the Effects of a Successful Phish
- Stop Threats Before they Reach the Inbox!
- Email Link Protection

Source: PhishProtection

Data Backups

- Backups are the Best way to Take Control of your Defense against Ransomware
- User & Personal Data Backups
- Server & Application Data Backups
- Cloud Services are Typically not Backed Up
- Backups are Great…but can you Recover?
- How to Protect Backups from Ransomware:
  - Keep Backups Offline (Tape or other Media)
  - Encrypt Backups
  - Increase Backup Frequency

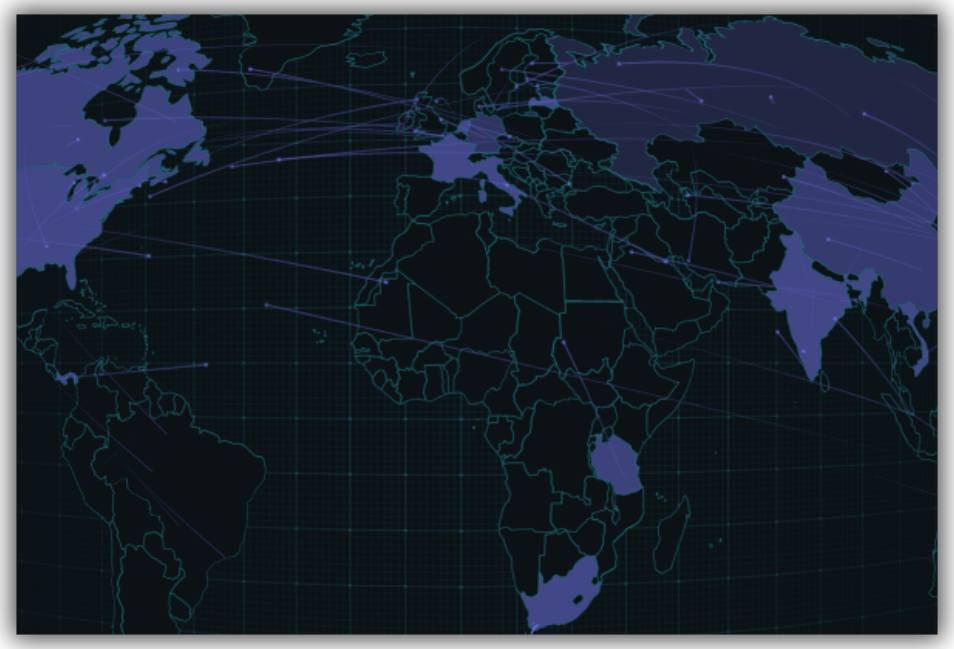
Sources: Darkreading.com and Redmondmag.com

PPAI ONLINE™ Education

Additional Resources

Note: These are case study examples and PPAI does not endorse any particular platforms or services.

- The Value of a Hacked Email Account
- Have I Been Pwned – Email Checker
- Have I Been Pwned – Password Checker
- Virus Attachment Scanner
- Live Threat Map



PPAI ONLINE™ Education

Q & A

DAVID JACKSON
Director of Information Technology
Sweda Company

MIKE PFEIFFER
VP of Technology
American Solutions for Business