The Ultimate

Employee Cybersecurity Training Checklist

INTRO TO CYBERSECURITY

- Overview of Cybersecurity
- Importance of Employee Involvement

UNDERSTANDING CYBER THREATS

- Types of Cyber Threats
  (Phishing, Ransomware, Social Engineering)
- Real-life Examples and Case Studies

RECOGNIZING PHISHING ATTEMPTS

- Identifying Suspicious Emails
- Verifying Sender Information
- Avoiding Clicking on Suspicious Links or Attachments

PASSWORD SECURITY

- Creating Strong Passwords
- Implementing Multi-Factor Authentication (MFA)
- Password Management Tools

SOCIAL ENGINEERING AWARENESS

- Recognizing Manipulation Tactics
- Verifying Identities in Communications
- Reporting Suspicious Activities

DEVICE SECURITY

- Securing Computers, Laptops, and Mobile Devices
- Regular Software Updates and Patches Antivirus and Anti-Malware Software

SAFE INTERNET BROWSING PRACTICES

- Avoiding Suspicious Websites
- Understanding the Risks of Downloads
- Using Secure Browsing Protocols (HTTPS)
- Content Filter to Block Suspicious Websites

DATA HANDLING AND PROTECTION

- Identifying and Protecting Sensitive Data
- Secure Data Transfer and Storage Practices (Data Loss Prevention / DLP)
- Secure Data Disposal

WI-FI SECURITY

- Securing Wi-Fi Connections
- Avoiding Public Wi-Fi for Sensitive Activities
- Understanding Risks of Unsecured Networks

EMAIL SECURITY BEST PRACTICES

- Verifying Email Sender Information
- Reporting Suspicious Emails
- Avoiding Opening Unknown Attachments or Links
- Implement Spam Filtering

CORNERSTONE TECHNOLOGIES

(269) 321-9442

CornerstoneisIT.com

The Ultimate

Employee Cybersecurity Training Checklist

PHYSICAL SECURITY MEASURES

- Protecting Devices from Theft or Unauthorized Access
- Proper Handling of Physical Documents

REMOTE WORK SECURITY

- Using VPNs for Secure Connections
- Secure Communication Tools
- Home Network Security

INCIDENT REPORTING PROCEDURES

- Establishing Clear Reporting Channels Reporting Security Incidents or Concerns Promptly

MOBILE DEVICE SECURITY

- Securing Smartphones and Tablets
- Enabling Device Encryption and Remote Wipe

USB SECURITY

- Exercising Caution with External USB Drives
- Scanning for Malware Before Use

SOCIAL MEDIA RISKS

- Awareness of Risks Associated with Sharing Information
- Adjusting Privacy Settings

DATA BACKUP PROCEDURES

- Regular Data Backup Practices
- Importance in Mitigating Ransomware Attacks

THIRD-PARTY SECURITY

- Evaluating and Ensuring Security Practices of Third-Party Vendors
- Securing Interactions with External Services

EMPLOYEE TRAINING AND AWARENESS PROGRAMS

- Regular Updates on Emerging Threats
- Simulated Phishing Exercises

CONCLUSION AND CONTINUOUS IMPROVEMENT

- Reinforcement of Key Takeaways
- Encouraging a Culture of Cybersecurity
- Continuous Learning and Adaptation to New Threats

CORNERSTONE TECHNOLOGIES

(269) 321-9442

CornerstoneisIT.com