CYBERSECURITY

EBERLY SYSTEMS

Security Awareness Training

Understanding cybersecurity principles can help safeguard your organization's sensitive information. Eberly Systems not only educates employees on security best practices but also fortifies the organization's overall cybersecurity posture, reducing the risk of breaches and fostering a culture of security awareness.

Why It Matters

Eberly Systems offers comprehensive security awareness training as part of their managed IT services to help:

- Reduce financial losses from fraudulent transactions
- Build trust with clients by prioritizing their security
- Protect your business from hackers exploiting weak points

Red Flags of Cyber Threats

- Unsolicited phone calls or emails requesting sensitive data or requests for immediate action on financial transactions
- Suspicious social media messages about work-related topics
- Too-good-to-be-true offers deals and or awards

What Cybercriminals Are After

Low-Value Data
Personal Information, including names, phone numbers, and addresses

High-Value Data
Banking details, IP addresses, confidential business designs, patents

Premium-Value Data
Credit card details or remote computer access

Cybersecurity Best Practices

1. **Strong Passwords & Multi-Factor Authentication (MFA)**
   - Use unique, strong passwords (16+ characters)
   - Store passwords in a password manager or securely offline
   - Enable MFA using app-based codes or physical security keys
2. **Protect Sensitive Information**
   - Classify data as public, internal, sensitive, or confidential
   - Avoid storing sensitive data in emails or unsecured files
   - Use encrypted storage and transmission methods
3. **Email & Social Engineering Awareness**
   - Be cautious of unexpected or urgent financial, legal, or tax-related emails
   - Use the SLAM Method (Sender, Links, Attachments, Message) to evaluate emails
   - Verify unusual requests through a secondary communication channel
4. **Safe Internet & Device Usage**
   - Use up-to-date version of major Web Browsers & avoid inputting sensitive information when given warning of "Not Secure" web pages
   - Avoid clicking on unknown links or downloading files from untrusted sources
   - Keep devices updated and install commercial security software
5. **Data Backup & Business Continuity**
   - Regularly backup data offline to prevent data loss
   - Ensure all Business Critical data is stored in an approved location, which is regularly backed up and tested by your I.T. team

Contact Us

(610) 374-4049

www.eberlysystems.com