THE 15 MOST EFFECTIVE TACTICS CYBERSECURITY AWARENESS CHECKLIST

SECURITY ASSESSMENT

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

□

EMAIL PHISHING

90% of breaches and compromises start with phishing attacks. These emails are becoming even harder to spot. We'll help train your staff and provide technical solutions to protect against these attacks.

□

PASSWORDS

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

□

SECURITY AWARENESS

Train and test your users – often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

□

ADVANCED ENDPOINT PROTECTION & RESPONSE

The latest in advanced endpoint security technology protects against file-less and script based threats and can even rollback a ransomware attack.

□

MULTI-FACTOR AUTHENTICATION

Utilize MFA whenever you can - on your network, email, mobile apps, banking, social media and other services your business uses. This ensures your data stays safe even if your password gets stolen,

□

COMPUTER UPDATES

Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

□

DARK WEB RESEARCH

Knowing in real-time what passwords and accounts have been posted on the Dark Web can allow you to prevent a data breach. We scan the Dark Web for your stolen credentials that may have been posted for sale.

□

SIEM / LOG MANAGEMENT

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

□

PHYSICAL SECURITY

This is often an overlooked piece of security programs. Keeping uninvited guests out of your office and securing areas is crucial to protecting sensitive data and your business from breaches.

□

MOBILE DEVICE SECURITY

Today's cyber criminals attempt to steal data or access your network by way of employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

□

FIREWALL

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call use today!

□

ENCRYPTION

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

□

BACKUP

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

□

CYBER INSURANCE

If all else fails, protect your income and business with cyber damage and recovery insurance policies.

□