Provided By Total Network TEK
www.TotalNetworkTEK.com
Call or Text 337-232-2525

INTERNET SECURITY

RECOMMENDED BEST PRACTICES

Email and Web Links

- Be cautious with unexpected emails, especially those requesting sensitive information or urgent actions.
- Verify the sender's identity by checking the email address for discrepancies and looking for signs of phishing, such as poor grammar. Verify with employees and clients any requested changes to payroll or payment requests directly.
- Always hover over links to preview the URL and ensure its legitimacy before clicking on them.
- Avoid entering your credentials through email links. Go directly to the website yourself via your browser instead of clicking on email links.
- When sending PII via email, use a secure and/or encrypted email.

Device Separation & External Storage Media

- Maintain separate devices for personal and professional use.
- Avoid performing business-sensitive tasks on personal devices.
- Do not connect unknown external storage devices (like USB drives) to company computers, as they may contain malware. Use only trusted and scanned media.

Software Downloads

- Download software only from official websites or trusted sources.
- Avoid third-party sites that may host compromised versions.

Windows and Software Updates

- Ensure that all updates for Windows and other software are kept up to date.

Antivirus & Pop-up Blocking Software

- Use business-grade antivirus software instead of free versions.
- Keep your antivirus program up to date to protect against malware and new threats.
- Ignore suspicious pop-up ads that may contain malware and use a reputable ad blocker to reduce risks.

Information Sharing

- Never disclose usernames, passwords, or client information to unverified sources.
- Report any solicitation for sensitive information to your supervisor immediately.

Password Policy

- Use complex passwords that consist of letters, numbers, and special characters, with a minimum length of 8 characters.
- Implement multifactor authentication for important systems.
- Change default passwords and update them periodically if multifactor authentication isn’t available.
- Do not write down or post passwords in easily accessible or visible locations.
- Use a secure password manager.

Online Practices

- Always use secure connections (HTTPS://) while browsing.
- Avoid using public Wi-Fi to access business email or sensitive information without a company-provided VPN.

Credit Card Information Security

- Use encrypted storage for credit card information and restrict access to trusted individuals only.
- Follow PCI DSS guidelines for compliance and safety.
- Do not store full credit card details in the same location.

Your attention to security is crucial for protecting sensitive information! Thank you for your diligence.