#SafeData: FoxNet Best Practices

There's no shortage of reasons to stay on top of data safety. From ransomware attacks to unexpected disasters, it's important to have a plan for #SafeData. But with technology changing rapidly, keeping your data safe can be overwhelming. How do you know which steps to take first?

FoxNet wants to help, and that's why we created this #SafeData checklist to help you cover all your security bases. Follow these steps, and you can be confident that you're covering all your security bases.

#SafeData Checklist

1. **Is your system security up-to-date?** Out-of-date system security is one of the most common vulnerabilities that malware and other online threats exploit. If it's been six months or more since your system security was updated, you're putting your data at risk every time you log on.

2. **Is your WiFi secure?** - Securing your WiFi with a password that's difficult for others to guess is important. If you fail to secure your WiFi, anyone in range with a laptop, phone, or other device can hop onto your network and use your connection to download potentially illegal files, view other devices using the network, and, if they're skilled, view your private data.

3. **Are you updating passwords and tiering access? -** Most of us know the importance of changing our passwords frequently. However, limiting password access to different layers of your business is also a great #SafeData practice. If your business uses multitier architecture, segregating presentation, application processing, and data management functions from each other, keep access to each tier password-protected, and only provide the passwords to those who need it.

4. **Is your data backed up in multiple locations?** When it comes to backing up your data, follow the **3-2-1 Rule.** To protect against unexpected disasters or security breaches, the #SafeData best practice is to always have 3 copies of your data, with 2 copies stored in separate storage units and 1 offsite. Many businesses choose cloud storage for their offsite backup location.

5. **How secure is your email infrastructure**? Email phishing scams occur when senders create email addresses or websites that appear to mimic a trusted sender or site to trick you into providing sensitive information, such as banking info. Many email infrastructures are sophisticated enough to recognize these emails as spam and flag them before they reach your inbox. If your email client is out-of-date and doesn't have high-quality spam detection, consider updating your email infrastructure to automate the process of weeding out unsafe senders.

6. Are you screening emails from unknown senders? No matter how secure you believe your email infrastructure is, be cautious about opening an email (especially an email containing any attachments) from an unknown sender. If you don't recognize the sender's domain name, type into your favourite search engine. Repeat offenders tend to make enemies, who will post about their experience with specific malicious senders online.

7. **Have you updated firewalls, antivirus, and anti-malware software**? Hackers create new, malicious online threats every day, so it makes sense that you'll need to update your antivirus and anti-malware software frequently to guard against the latest malware and ransomware threats. Ransomware attacks occur when a hacker takes your data hostage and encrypts it, making it impossible for you to access. Typically, hackers hold the data hostage in exchange for fees, payable in bitcoin. One of the best ways to prevent an attack like this is to keep your threat databases up to date.

8. **Are you using a monitoring or detection software?** Many trustworthy products can do the majority of system monitoring and detection of threats for you. ZeroSpam provides cloud-based email security, which detects phishing scams, while eSentire provides system-wide security monitoring.

Most IT resources are spent simply maintaining a business's infrastructure? FoxNet Managed Services can simplify the day-to-day running of your IT, including data security precautions.