PROTECT YOUR BUSINESS

CYBERSECURITY: TOP TASKS

There was a cyberattack roughly every 39 seconds in 2022. That means more than 2200 attacks daily. Protect your business with these best practices.

UPDATE YOUR SOFTWARE

Software companies offer new versions not only to update features but also to fix known bugs and upgrade security. Don't ignore those update notifications, as they could include valuable protection.

ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Add an extra layer of protection by requiring added information to verify identity on top of the username and password. It limits potential compromise.

CHECK LINKS BEFORE YOU CLICK

What you see may not be what you get. Hover over the target URL of the link to see where it is going before clicking.

DOUBLE CHECK SITES FOR HTTPS

Only encrypted websites will be marked HTTPS by most browsers. This marks the site as more trustworthy and secure. Don't enter data on HTTP-only site.

USE STRONG PASSWORDS

Creating more complex passwords takes a little more effort. With password managers, you don't have to worry about remembering stronger credentials. Plus, you can avoid repeating passwords across accounts.

AVOID PUBLIC NETWORKS

Wi-Fi hotspots offer convenience, but you sacrifice security. A public connection could be unencrypted, hijacked, or leave you vulnerable to malware, viruses, and log-in credential theft.

BACKUP DATA

Back up important data at least weekly, or even daily. This can protect your data from malicious action, natural disasters, or other accidents that cause data loss.

SCAN EXTERNAL DEVICES FOR VIRUSES

External storage devices can be infected with malware. Scan known devices before connecting. **NEVER** connect unknown devices to your computer.

DON'T LEAVE DEVICES UNATTENDED

Always keep your devices with you to prevent loss or theft. Plus, you'll avoid thieves accessing your passwords or other important or confidential data.

PROTECT MOBILE DEVICES

Keep your device's operating system up to date. Lock your device with a PIN and use data encryption where possible. Also, install only apps from trusted sources.

HAVE A RISK MANAGEMENT PLAN

A cybersecurity plan covering strategy and procedures and outlining how your business will react to attacks can help you cut risk and react more quickly.

EDUCATE EMPLOYEES

According to Verizon, 82% of breaches involve human errors or misuse. Teach employees about basic cybersecurity and ensure they consistently follow best practices to reduce your risk.

Take action. No matter your business size or industry, you are always a target to hackers.

XSolutions.com / contactus@xsolutions.com / (845) 362-9675