DIGITAL SPRING CLEANING CHECKLIST FOR SMBs

BROUGHT TO YOU BY: NATIONAL CYBERSECURITY ALLIANCE BBB

Millions of Americans nationwide will devote warm weather weekends to sprucing up their homes for spring. If you are a small to medium-sized business (SMB), the National Cyber Security Alliance (NCSA) and the Better Business Bureau (BBB) have some tips to protect your business and your customers' data. A few proactive steps to declutter, get organized and establish good practices will help safeguard your business against disruptive issues, which can cause chaos if your company's data is compromised.

GET STARTED BY INITIATING THE FOLLOWING TOP "TAKE-ACTION TIPS":

- [ ] **Lock Down Your Login:** Security is critical to protecting your customers' and employees' personal data. One of the first things everyone needs to do is ensure that passphrases are lengthy, unique and safely stored. In addition, it is essential to fortify accounts by adopting strong authentication, which adds another layer of protection.
- [ ] **Update Your System and Software:** Don't procrastinate any longer! Having the latest updates, security software, web browser, and operating system is one of the easiest ways to keep devices secure and protect data. This simple "digital to do" will help keep cybercriminals at bay.
- [ ] **Back It Up:** Protect your workplace data by making copies – or backups – of your most important files. Whether it's your vendor database, employee contact information, or customer financial data, back up your files this spring and set a schedule to do so regularly.

To keep your business safe and secure, NCSA and BBB recommend establishing, communicating and continuously updating policies and procedures to aid in protecting your business from unforeseen cybersecurity and privacy issues.

DIGITAL SPRING CLEANING CHECKLIST FOR SMBs

KEEP A CLEAN MACHINE

- [ ] **Update the software on all of your company's devices** – including point of sale systems and IoT (Internet of Things) devices.
- [ ] **Establish or update BYOD (Bring Your Own Device) policies** to limit the amount of risk that can be brought into the organization from employee-owned and controlled devices.
- [ ] **Delete software and apps you are no longer using.**
- [ ] **Teach employees good habits** when it comes to maintaining clean and secure devices

DIGITAL FILE PURGE

- [ ] **Establish and communicate records retention guidelines** for your digital and physical records. Permanently and securely dispose of all old or unnecessary data.
    - o See the BBB tips below for the proper disposal of electronically stored information.
- [ ] **Clean out your old email** and empty deleted folders. If you need to keep old messages, move them to an archive.
- [ ] **Unsubscribe** from newsletters, email alerts, and updates you no longer read.
- [ ] **Use the 3-2-1 rule to back up your business data: 3** backup copies, **2** different media types, **1** offline and in a separate location.
- [ ] Check to see if there is a BBB Secure Your ID Day or similar event in your area. Many "shred day" events include safe destruction of electronic equipment and files, as well.

DIGITAL SPRING CLEANING CHECKLIST FOR SMBs

CLEAN UP YOUR ONLINE PRESENCE

- [ ] **Own your online presence** by reviewing the privacy and security settings on accounts you use. You should do this for both business accounts and personal accounts.
- [ ] **Control your role** by reviewing and limiting who has administrative access to your online accounts. Grant access only to individuals who **need** it to complete their assigned job responsibilities. Allocate data access privileges based upon job duties, not job titles.
- [ ] **Clean up your social media presence** by deleting old or unnecessary photos and by deleting accounts no longer in use.
- [ ] **Take care with what you share** by updating or creating policies and procedures for what content should be/can be shared on your business social media accounts.
- [ ] **Web browsers should be updated** to the most current versions for all internet-connected devices. Don't forget those devices beyond the office walls that remote or distributed workforces utilize.

DUST OFF THE PLAN

- [ ] **Cybersecurity should be part of any organization's continuity planning.** Just as you conduct fire drills to test your organization's fire response strategy, take time this spring to convene a cross-functional team to review your cybersecurity strategy. What are the most valuable assets you need to protect? How do you plan to protect those assets? How does the organization intend to detect vulnerabilities or breaches? How does the organization propose to respond to and recover from a cyber incident?

BBB has established user-friendly guidelines to help you with the safe disposal of electronically stored data. Be sure to prep your data in advance of participating in BBB's Secure Your ID Day:
Know what devices to digitally "shred": Computers and mobile phones aren't the only devices that capture and store sensitive, personal data. External hard drives and USBs, tape drives, embedded flash memory, wearables, networking equipment, and office tools like copiers, printers, and fax machines all contain valuable personal information and stored images.

- ☐ **Clear out stockpiles:** If you have a stash of old hard drives or other devices – even if they're in a locked storage area – information still exists and could be stolen. Don't wait: wipe and/or destroy unneeded hard drives as soon as possible.
- ☐ **Empty your trash or recycle bin on all devices, and be certain to wipe and overwrite:** Simply deleting and emptying the trash isn't enough to completely get rid of a file. You must permanently delete old files. Use a program that deletes the data, "wipes" it from your device and then overwrites it by putting random data in place of your information – that then cannot be retrieved.
    - o Various overwriting and wiping tools are available for electronic devices. For devices like tape drives, remove any identifying information that may be written on labels before disposal, and use embedded flash memory or networking or office equipment to perform a full factory reset and verify that no potentially sensitive information still exists on the device.
- ☐ **Decide what to do with the device:** Once the device is clean, you can sell it, trade it in, give it away, recycle it, or have it destroyed. Note the following:
    - o **Failed drives still contain data:** On failed drives, wiping often fails, too; shredding/destruction is the practical disposal approach for failed drives. Avoid returning a failed drive to the manufacturer; you can purchase support that allows you to keep it – and then destroy it.
    - o **To be "shredded," a hard drive must be chipped into small pieces:** Using a hammer to hit a drive only slows down a determined cybercriminal; instead, use a trusted shredding company to dispose of your old hard drives. Device shredding can often be the most time- and cost-effective option for disposing of a large number of drives.

SMBs can learn more about online safety with NCSA's CyberSecure My Business™ or BBB's "5 Steps to Better Business Cybersecurity" (BBB.org/cybersecurity).

CyberSecure My Business™ – of which FedEx is a Founding Partner, Trend Micro is a Signature Sponsor and Infosec is a Contributing Sponsor – was created to help protect the SMB community's cybersecurity. It does so by offering free interactive training workshops, webinars and monthly newsletters summarizing the recent hot topics.

Receive the latest cybersecurity news and resources for small businesses by signing up for the CyberSecure My Business™ Newsletter.

StaySafeOnline.org

National Cyber Security Alliance

@StaySafeOnline

BBB.org

Better Business Bureau

@BBB_US