BBB: Tip – Give yourself a Spring digital makeover

Posted on Wednesday, Apr 7, 2021

>> WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. Get the app or access via desktop.

CONTACT:	**Lisa Schiller, Media Relations**
PHONE:	**414- 847- 6055**
FAX:	**414-302- 0355**
E-MAIL:	**lschiller@wisconsin.bbb.org**

Milwaukee, Wis. – The weather is breaking in some parts of the country, inspiring people to clean up or clean out the clutter. The one area many people overlook isn't the corner of a room or a forgotten closet, it's probably the digital device you're reading this article on. It's the same one you use to shop, scroll through social media, do your banking, and maybe even do some work on for your job. The National Cyber Security Alliance (NCSA) and the Better Business Bureau (BBB) remind everyone that when clearing out the physical clutter, there's probably a bunch of digital data clutter that lives on your electronic devices.As businesses and their employees switched over to working from home in the last year, the focus on cybersecurity and protecting sensitive information became critical. NCSA has advice on how to keep this information safe.

Just in case there are a few extra hours or minutes of the day, it may also be a good time to give yourself a digital makeover. Taking some simple, proactive steps will go a long way in safeguarding against any number of potentially disruptive issues – like identity theft, loss of funds, or credit card fraud – that can cause mayhem by compromising your data. Take the time to put into practice a few precautionary measures and you will have greater peace of mind – not only this spring but all year round.

NCSA and BBBs nationwide are encouraging people to check their smartphones, laptops, and tablets and a few minutes to review these tips.

- **Lock Down Your Login:** Security is critical to protecting accounts being used for work and for home. Ensure passphrases for each account are lengthy, unique, and safely stored. Enable 2-factor authentication on all accounts that offer it.
- **Update Your System and Software:** Avoid procrastination! Having the most current software, web browsers, and operating systems are some of the easiest and fastest ways to protect your most sensitive assets.
- **Back It Up:** Protect your personal and workplace data by making electronic copies – or backups – of your most important files. Use the 3-2-1 rule to help guide you: 3 backup copies, 2 different media types, 1 offline and in a separate location.
- **Clean Up Your Online Presence:** When was the last time you used all of the apps on your phone or tablet? Do you know what the settings are on all of the social media accounts that check-in with friends and family? These are questions to ponder and settings to review while checking these accounts. Then, control your role by making sure you know who has administrative access to your online accounts. Keep all of your passwords private.
- **Be careful What You Share**: Quizzes are fun and keeping in touch is a necessity these days. However, watch out for apps and questions that might give away too much information about you, your location or your family.

In addition to following the above-listed tips, small business owners should take time in establishing, updating, and communicating policies and procedures around many topics such as record retention, etc. It is also imperative that a cybersecurity strategy is in place and utilized by all employees. BBB has tips on BBB.org/smallbusiness when it comes to avoiding online scams when working from home.

BBB Secure Your ID Day

Did you know that protecting your identity is largely in your own hands? Many identity theft victims can trace the theft to something that was stolen from their own possession. BBB has a few guidelines to help safely dispose of electronically stored data. Be sure to prep your data in advance of participating in BBB's Secure Your ID Day or other shredding events.

- **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 – which then cannot be retrieved.
- 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:
- **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.
- **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.

Additional Resources:

BBB.org/Secure-Your-ID-Day: information on shredding events and tips on what to save and for how long.

BBB.org/Cybersecurity for "5 Steps to Better Business Cybersecurity."

BBB.org/smallbusiness for resources concerning the COVID-19 crisis.

BBB.org/coronavirus for general information and tips.

StaySafeOnline.org for tips from the National Cyber Security Alliance and the Canadian Centre for Cybersecurity

Federal Trade Commission's guides for disposing of your computer or mobile device and e-waste advice from the Government of Canada.

IdentityTheft.gov for a customized recovery plan if you have been the victim of identity theft.

Internal Revenue Service advice for taxpayers to protect personally identifiable information (PII) that can be used for identity theft.

IRS tips for employers and tax preparers to protect employee and customer data.

For more information or further inquiries, contact the Wisconsin BBB at www.bbb.org/wisconsin, 414-847-6000 or 1-800-273-1002. Consumers also can find more information about how to protect themselves from scams by following the Wisconsin BBB on Facebook, Twitter, Instagram and YouTube.