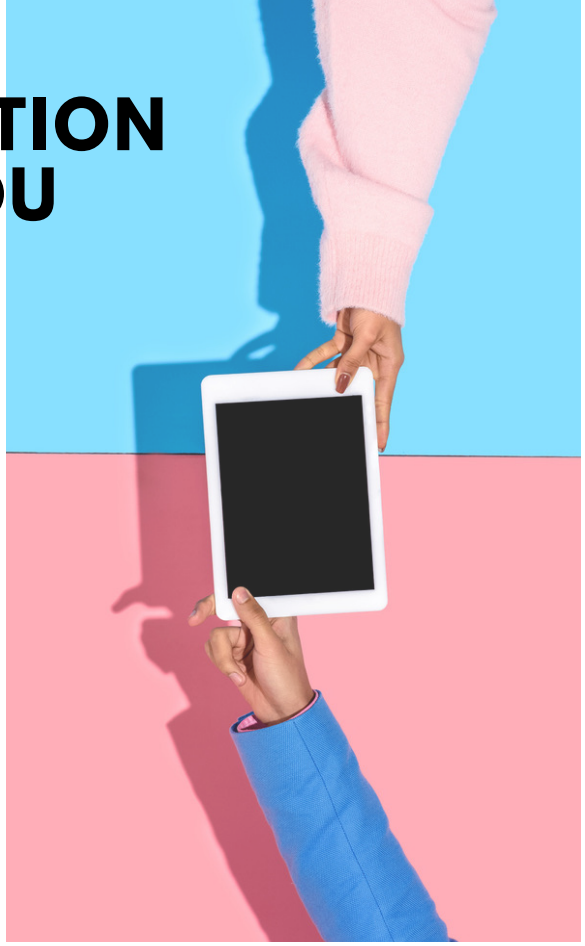
TOP ONLINE "TAKE-ACTION TIPS" TO HELP KEEP YOU SAFE AND SECURE



BROUGHT TO YOU BY

NATIONAL CYBERSECURITY ALLIANCE

BBB

When you are sprucing up your home this spring, the National Cyber Security Alliance (NCSA) and the Better Business Bureau (BBB) encourage everyone take a few minutes to tend to your digital life and safeguard your personal information with these Take-Action Tips.

LOCK DOWN YOUR LOGIN

Both at home and at work, security is critical to protecting highly personal accounts. 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 personal and workplace data by making electronic copies or backups of your most important files. Whether its family photos, health records or employee contacts, **back up your files** this spring and set a schedule to do so regularly throughout the year.

Since the tax filing season is finally behind us, many plan to purge both paper and electronic files. BBBs across the country will host **Secure Your ID Day** events on Saturday, April 27 to assist with the safe disposal of your most personal records. To ensure that digital devices are prepped, follow these tips below.

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, USBs, tape drives, embedded flash memory, wearables, networking equipment and office tools like copiers, printers and fax machines all contain valuable personal information.

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.

- 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, 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.

NATIONAL CYBERSECURITY ALLIANCE

StaySafeOnline.org

@StaySafeOnline

BBB

BBB.org

@BBB_US