

## DATCP 2015 Cyber Security Awareness Month Daily Tips

### **Thursday, 10/1. Fresh start for the month – change your passwords frequently**

Cyber Security Awareness Month, Tip #1: New month...new passwords

It's the first of the month! Change your online passwords today and use a long combination of numbers, letters and special characters. For best protection, do this on a regular basis, and keep a totally different password for your email. Why? You'll find out here tomorrow! [#CyberAware](#)

### **Friday, 10/2. Protect your email account**

Cyber Security Awareness Month, Tip #2: Protect your email account

Remember yesterday when we said to use a completely different password style for your email versus what you use for your other online accounts?

Many websites send password update and account access emails to consumers, so getting a hold of these emails could potentially give a hacker access to all of your online accounts. Your email password should be the toughest to decode. [#CyberAware](#)

### **Saturday, 10/3. Run a free computer security check**

Cyber Security Awareness Month, Tip #3: Run a free computer security check

Happy Saturday! Start out CSAMonth with a clean sweep of your computer system. At the end of the month, sweep it again and make a plan to do so regularly.

[StaySafeOnline.org](http://StaySafeOnline.org) has a listing of free, trusted security check services here:  
<https://www.staysafeonline.org/sta.../free-security-check-ups/>. [#CyberAware](#)

### **Sunday, 10/4. Backup your contacts, photos, videos, music, documents and more**

Cyber Security Awareness Month, Tip #4: Backup, backup, backup

Halloween is scary. But do you know what's scarier? Losing all of your important files and your collection of photos, music and videos. It happens and it's awful...unfortunately, I know from experience. Don't let it happen to you.

Regularly sync your mobile devices with your laptop or desktop computer or to a cloud service. Backup your laptop or desktop to an external hard drive or cloud service. One dead hard drive, misplaced mouse click or lost device could spell the end of all of your files...take steps NOW to protect your data. [#CyberAware](#)

### **Monday, 10/5. Ransomware**

Cyber Security Awareness Month, Tip #5: What is "ransomware?"

“Ransomware” is a particularly nasty type of computer virus that can lock up your system and files until you pay the offenders a ransom. The message that takes over your screen may falsely claim to be from the FBI or the U.S. Dept. of Justice saying that you visited illegal online contact.

If you pay a ransom to “unlock” your computer, your system will still likely be carrying some form of malware. The federal Internet Crime Complaint Center (IC3) recommends that victims not pay any money or provide personal info to the criminals to free up their system. Instead, contact a local, trusted computer tech service for help.

Remember yesterday’s backup tip? Ransomware can destroy your files. Always backup your data for safekeeping. [#CyberAware](#)

BONUS cyber tip for today: Our friends at ReadyWisconsin have a Cyber Security Awareness Month page up at <http://www.readywisconsin.wi.gov/cyber/default.asp>. Check it out for more great cyber safety tips. They are also on Facebook at [ReadyWisconsin!](#)

## **Tuesday, 10/6. Use caution on public networks**

Cyber Security Awareness Month, Tip #6: Use caution on public networks

If you are using a public Wi-Fi hotspot to connect to your personal accounts on a mobile device, limit the types of business you conduct, shield your typing from prying eyes, and set your device to hide your password character entries. Hold off on using online banking websites or sites that require sensitive personal information (like Social Security numbers) until you are on a secure private network or a home computer. [#CyberAware](#)

## **Wednesday, 10/7. Bluetooth risks**

Cyber Security Awareness Month, Tip #7: Bluetooth risks

Bluetooth has hit the big time, giving us a means of taking hands-free calls, wirelessly transferring files, and streaming music to our stereos. But Bluetooth has long been vulnerable to security exploitation. “Bluejacking,” “Car Whisperer” and “Bluebugging” are all forms of Bluetooth threats (look them up...they’re both interesting and troubling).

The only safe way to avoid these risks is by turning off Bluetooth features entirely when they are not in use (and not just putting them in “undetected” mode). Many battery management applications can help automate this process. Also, keep your device’s operating system up to date for the best overall security protections. [#CyberAware](#)

## **Thursday, 10/8. Location Services**

Cyber Security Awareness Month, Tip #8: Tag, you’re it! And in trouble.

“Geotagging,” or linking GPS coordinates with your photos and online posts, is often turned “on” as a preset on mobile devices. Be very careful how you utilize this feature...this information can give criminals the tools they need to track or rob you.

Don't geotag pictures of your home or children and pay attention to which applications use the feature in your device and app settings. [#CyberAware](#)

### **Friday, 10/9. Microsoft Tech Support scams**

Cyber Security Awareness Month, Tip #9: Computer tech support scams

If you receive a call out of the blue claiming that your computer has a virus and that the caller can help you get rid of it, hang up immediately. It's a scam. The callers often falsely claim to represent Microsoft or a local tech support company to gain the consumer's trust. They tell the consumer that they can remove the (non-existent) virus from their computer for a fee. The caller asks the victim to download software from the internet that grants them remote access to the system.

If you allow these scammers to access your computer, they can load any number of malicious software programs onto your machine and they may access your files as well. If you give them your credit card number to pay for their "services," you can expect to get ripped off there too. This is typically a phone-based scam, but also shows up in online pop-up messages saying you have a computer virus and telling you to call them for help. Don't do it. [#CyberAware](#)

### **Saturday, 10/10. Email/text spam/scams**

Cyber Security Awareness Month, Tip #10: Email and text message spam and scams (say that three times fast!)

The terms "scam" and "spam" are almost interchangeable when it comes to email and text messages. Spam messages are junk bulk emails or texts that you receive without permission. The senders may be hocking get rich quick schemes and questionable products or they could be looking to get you to turn over personal or credit information. Either way, you're ripped off. Did we mention that the messages can also transmit malware?

Simply put, if you get an odd email or text out of the blue, delete it and take no further action. There is a lot to cover on email and text spam, so your best resource is our DATCP fact sheet:

<http://datcp.wi.gov/uploads/Consumer/pdf/Spam284.pdf> [#CyberAware](#)

### **Sunday, 10/11. Government impostor scams**

Cyber Security Awareness Month, Tip #11: Government impostor email and phone scams

Many criminals are using government agency names or "look-alikes" in recent email and phone scams, hoping to add legitimacy to their ploys. Have you gotten a threatening call demanding money from someone claiming to be with the IRS? That's a regularly used con. Did you get an email from "State Court" about a required appearance? That's another one (do NOT open the attachment in that email!).

Don't fall for these scams. Delete the emails and hang up on these callers. They want your money, your personal information, or to infect your computer with malware. If you question the legitimacy of a communication from a governmental agency, contact DATCP's Consumer Protection Hotline (800-422-7128) or call the misrepresented agency directly to inquire. [#CyberAware](#)

**Monday, 10/12 (\*start of mobile device week). Have you accounted for all of the mobile devices in your household? Are they all up to date?**

Cyber Security Awareness Month, Tip #12: Where are all of your web-enabled devices?

Here is a simple but important family exercise: where are all of your family's smartphones, tablets, laptops, desktops, smart TVs, etc.? Being able to account for all of the web-enabled devices in your household is a great first step in ensuring that your family members' personal information is safe.

Step two: now that they are accounted for, protect your devices. Update the operating systems and antivirus software on your devices in order to protect against recent viruses and to patch any holes that hackers can use to access your systems. [#CyberAware](#)

**Tuesday, 10/13. Device passwords**

Cyber Security Awareness Month, Tip #13: Mobile device passwords

Most smartphones and tablets require users to enter passcodes to access the device. It may be a minor inconvenience, but it's hard to argue how valuable that extra security step is...our mobile devices carry an incredible amount of info about us.

Use a unique passcode for each device. For added security, set your device to require regular password entries and use the fingerprint reader on newer devices for unlocks. We'll address mobile device safety further in tomorrow's tip. [#CyberAware](#)

**Wednesday, 10/14: Mobile device lock out/tracking**

Cyber Security Awareness Month, Tip #14: Lost phone? Bad. Lost data? Worse.

If your smartphone or tablet is lost or stolen, you want to have a fighting chance at finding it or at least at wiping out any personal data before it's accessed by the wrong party. For this purpose, there are tracking applications either built in or available by download for all of the major mobile device operating systems.

If you are a Google Android user, your device includes Android Device Manager. Apple's devices include Find My iPhone. Using these features, you can remotely locate your device or lock or erase your device...but you need to make sure these features are active and properly set up before you run into trouble. Read up on these services and make sure they are running on your devices. [#CyberAware](#)

**Thursday, 10/15: Jailbreaking puts you at risk**

Cyber Security Awareness Month, Tip #15: "Jailbroken" devices pose risks

"Jailbreaking" a device involves altering the native operating system in order to unlock capabilities within the device or to download unauthorized apps. Jailbreaking a device undermines and may disable the device's built-in security features. Malware-laden apps for jailbroken phones were at the heart of a recent hack of an estimated 225,000 Apple ID accounts.

Jailbreaking creates a number of additional risks: the device could be “bricked” or unable to operate, your manufacturer’s warranty could be voided, and the third-party apps you choose to download may contain malware. Is it worth the risk? That’s for you to decide. [#CyberAware](#)

### **Friday, 10/16 (\*end of mobile device week): Always keep your devices in a secure location**

Cyber Security Awareness Month, Tip #16: Keep an eye on your devices

Kind of a simple, self-explanatory tip today, but always keep your mobile devices with you in public and never leave them out “just for a couple of seconds.” A couple of seconds is long enough for a thief to disappear with your expensive device and your even more valuable data like contacts, messages, schedules, photos, music and more.

Earlier in the week we suggested tracking down and updating all of your family’s online devices. Now that they are accounted for, keep an eye on them in public and keep them locked up when not in use. [#CyberAware](#)

### **Saturday, 10/17: Three terms to know: phishing, smishing and cramming**

Cyber Security Awareness Month, Tip #17: Phishing, Smishing and Cramming

It’s Saturday, the Badger game is over (go Bucky!), and you have a spare couple of seconds to read and learn, right? Here are three terms related to cybercrime that you need to know:

**PHISHING** – Pronounced like “fishing” and similar to fishing, digging or gathering. Internet scammers are often phishing for your personally identifiable information such as your Social Security number and date of birth, or your bank account information and credit card number. If you receive an unsolicited email from someone claiming to represent a legitimate organization and they ask for sensitive information – be careful. This is most likely a scammer trying to deceive you. In addition to compromising your financial information, phishing can also lead to identity theft.

**SMISHING** – This is a newer spinoff of phishing. Scammers use SMS (short message service) text messaging to try and convince consumers to give out personally identifiable information. Smishing poses the same risks as phishing, but tends to target younger consumers who make their cell phone numbers public through online social sites like Facebook or Twitter. Parents should talk to their children about the dangers of sharing personal information with strangers.

**CRAMMING** – This is the term used to describe unauthorized charges to your telephone bill. Examples of unauthorized charges could include voice mail, call waiting or a personal 800 number. Malicious smartphone apps, text messages, and email scams could set you up for these fees. Consumers need to closely monitor their monthly bills. You can contest charges for services you did not request. However, unless you look for them, you could unknowingly be paying for extras. [#CyberAware](#)

### **Sunday, 10/18: Identity Theft**

Cyber Security Awareness Month, Tip #18: Keep personal info personal

This is a great tip throughout the year and it shows up in nearly all of our scam warnings: Never give out personal or banking information on an unsolicited call or in response to an unsolicited email or text message. Period. It's that simple.

By acquiring just a small amount of information, identity thieves can destroy a person's financial reputation and cause endless stress on a person and their family. Identity theft costs consumers millions of dollars in fraudulent charges each year, and can take years and cost thousands of dollars to recover from. Please guard your personal information and keep it to yourself.

If you think you may be a victim of identity theft, contact DATCP's Office of Privacy Protection at 608-224-5163 or by visiting [privacy.wi.gov](https://www.privacy.wi.gov). [#CyberAware](https://twitter.com/CyberAware)

### **Monday, 10/19: Two-factor authentication**

Cyber Security Awareness Month, Tip #19: Use two-factor authentication when available

Two-factor authentication is a security process in which you provide two means of identification in order to log into a system – something you have and something you know. Something you have is typically a physical token, such as a fob, fingerprint or a code sent to your smartphone. Something you know is something memorized, such as a personal identification number (PIN) or a password.

When you use your credit card at the gas pump, you already do this. You swipe your card (something you have) and enter your ZIP code (something you know). So if one of your favorite websites strengthens its security features and offers to send you an additional passcode for logging in, take them up on it. [#CyberAware](https://twitter.com/CyberAware)

### **Tuesday, 10/20: Careful of info on social media websites – grandparent scams; thieves**

Cyber Security Awareness Month, Tip #20: Think before you post

Your fun-filled vacation photos could cause your grandma to get ripped off.

Why? Criminals can use the information you share on social media sites to create a narrative that they weave into their scams.

Consider the infamous "grandparent scam," where elderly citizens are called by a scammer claiming to be the person's grandchild. The "grandchild" says they are on vacation, were in an accident, and need an immediate wire transfer to get out of jail or the hospital. Your social media account could provide a tremendous amount of info for a scammer to use in their script, such as your name, family members' names, where you live and if you are away from home.

Remember those fun-filled pics I mentioned? By viewing your profile, the scammer knows you are away on vacation in \_\_\_\_ with your best friend \_\_\_\_\_. They can fill in the blanks, making for a much more believable con.

It's OK to share with friends and family on social media, but adjust the privacy settings for your accounts to block your content from strangers. Also, remember that sensitive information such as names, birth dates and Social Security numbers posted to social media accounts can be used by scammers to steal your identity. [#CyberAware](https://twitter.com/CyberAware)

### **Wednesday, 10/21: Think before you app**

Cyber Security Awareness Month, Tip #21: Think before you app

Malware lurks in downloadable applications. Only download software from authorized app stores – and even then, do some research about specific applications and developers before you make a purchase. Even apps as simple and seemingly harmless as a flashlight utility have been found to harvest and send data to advertisers without informing the user.

Before downloading a mobile app, understand what information (your location, access to social networks, etc.) the app accesses when running. You may be surprised at what you find. [#CyberAware](#)

### **Thursday, 10/22: Think before you act**

Cyber Security Awareness Month, Tip #22: Think before you act

Ignore unsolicited emails, phone calls or text messages that create a sense of urgency and require you to respond immediately to a problem...particularly one involving your bank account or taxes. This type of message is likely a scam. When in doubt, don't respond.

If you question the legitimacy of a message that claims to be from a business or government agency, call the organization directly to inquire. [#CyberAware](#)

### **Friday, 10/23: Sensitive transactions over secure WiFi**

Cyber Security Awareness Month, Tip #23: Is that website secure?

Here's a quick, easy tip: Before you enter personal or banking information into a website, make sure the URL starts with "https" rather than "http." The "s" stands for secure. Cool, right?

That was so quick...here's a Friday freebie: the tiny arrow next to the gas pump icon in your car's instrument panel tells you which side of the car the gas cap is on. Whoa. [#CyberAware](#)

### **Saturday, 10/24: Delete when done**

Cyber Security Awareness Month, Tip #24: Delete when done.

Many of us download apps for specific purposes (such as planning a vacation) and no longer need them afterwards. Or we may have previously downloaded apps that are no longer useful or interesting to us. It's a good security practice to delete all apps you no longer use. [#CyberAware](#)

### **Sunday, 10/25: WiFi/Bluetooth tracking**

Cyber Security Awareness Month, Tip #25: Now you see me, now you don't

You are a target for ads. Some stores and other locations look for devices with WiFi or Bluetooth turned on in order to track your shopping habits while you are within range. To avoid this tracking, disable WiFi and Bluetooth when not in use (and it will help you save battery life!). [#CyberAware](#)

### **Monday, 10/26: Protecting your kids**

Cyber Security Awareness Month, Tip #26: Take active steps to protect your kids BEFORE they log on

Keep your home computer in a central location where you can monitor your children's online usage.

Look for any protection features that are built in to the websites and software that your kids access and adjust them accordingly.

All major Internet service providers (ISPs) and cellular providers have tools to help you manage children's online experiences (e.g., selecting approved websites, monitoring the amount of time they spend online, or limiting the people who can contact them).

For these tips and much more, visit the "Raising Digital Citizens" page on the [StaySafeOnline.org](https://www.staysafeonline.org/.../f.../raising-digital-citizens) site: <https://www.staysafeonline.org/.../f.../raising-digital-citizens> [#CyberAware](#)

### **Tuesday, 10/27: Wipe data on your old phone before you donate, resell or recycle it**

Cyber Security Awareness Month, Tip #27: Wipe data before you upgrade

Looking to swap out for the latest smartphone? If you are trading in your phone at a retail store, the business will likely transfer your contacts to your new phone and wipe your data off your old phone. That's great. But what if you intend to donate, resell or recycle your old phone?

Before you turn your old phone over to anyone or throw it in a donation bin, you must remember to completely erase your data and reset the phone to its initial factory settings. Check your phone's general settings for a factory data reset option. If you don't know where to go, search online for info about your specific phone model or check with your cellular provider. [#CyberAware](#)

### **Wednesday, 10/28: online rental scams**

Cyber Security Awareness Month, Tip #28: That amazing, unbelievable online rental ad? Beware.

As always, if it's too good to be true, it probably is. If you are looking online for a rental property and find an unreal deal, be very, very cautious.

Scammers use information from real estate listings to post fraudulent apartment or home rental ads on Craigslist and other online sites. They may "rent out" a property that they don't own to multiple people, taking security deposits and first month's rents from all of these parties. Their listings may also be ploys to get you to pay for a credit report service...the scammers get a commission if you do.

Craigslist offers these two simple tips on their website: "Do not rent or purchase sight-unseen – that amazing 'deal' may not exist" and "Refuse background/credit checks until you have met landlord/employer in person." [#CyberAware](#)

### **Thursday, 10/29: About IC3**

Cyber Security Awareness Month, Tip #29: Get informed with IC3

We mentioned IC3 (the Internet Crime Complaint Center) in our cyber tip way back on 10/5. IC3 is a partnership between the FBI and the National White Collar Crime Center. If you have an interest in keeping up with the latest in major cybercrimes or if you want to file a complaint about an Internet crime, this website is an excellent resource: [www.ic3.gov](http://www.ic3.gov) [#CyberAware](#)

### **Friday, 10/30: DATCP Consumer Alerts**

Cyber Security Awareness Month, Tip #30: Stay informed with DATCP Consumer Alerts

You are already on our Facebook page, so you have an interest in cybercrime and consumer protection information. Great! But have you signed up to receive our Consumer Alerts by email or text?

Visit [DATCP.wi.gov](http://DATCP.wi.gov). Click the envelope icon in the left hand column that reads "Sign up here for email updates." Enter your email or text preference and email address or wireless number. Choose "Consumer Alerts" from the Consumer Protection group and any other DATCP email groups you would like to join. Click "Submit" at the bottom of that page. That's it! Now you won't miss any of our important scam alerts.

Consumer Alerts are also posted to the DATCP website here:

[http://datcp.wi.gov/Consumer/Consumer\\_Alerts/index.aspx](http://datcp.wi.gov/Consumer/Consumer_Alerts/index.aspx) [#CyberAware](#)

### **Saturday, 10/31: FBI Internet fraud tips**

Cyber Security Awareness Month, Tip #31: Happy Halloween, Boils and Ghouls!

Thanks for joining us throughout October for our daily cyber tips! Let's keep it simple but useful today...here is a list of tips from the FBI to protect you and your family from a number of forms of Internet fraud: [https://www.fbi.gov/scams-safety/fraud/internet\\_fraud](https://www.fbi.gov/scams-safety/fraud/internet_fraud)

Looking for more info? [DATCP.wi.gov](http://DATCP.wi.gov) is a great place to start (of course!), and check out [StaySafeOnline.org](http://StaySafeOnline.org) and [Consumer.ftc.gov](http://Consumer.ftc.gov) to keep you safe both this month and throughout the year. [#CyberAware](#)

###

(These daily tips were distributed by the Wisconsin Department of Agriculture, Trade and Consumer Protection through email and were posted to the agency's webpage and Twitter account and the Bureau of Consumer Protection's Facebook page.

For questions about these cyber tips or other Bureau of Consumer Protection communications, please contact Jerad Albracht, Senior Communications Specialist, 608-224-5007 or [jerad.albracht@wisconsin.gov](mailto:jerad.albracht@wisconsin.gov).)