

October is...  National Cybersecurity Awareness Month

STOP.THINK.CONNECT™

A NATIONAL CYBERSECURITY AWARENESS CAMPAIGN


Protecting Yourself and Your Family Online


 **UW Extension**
University of Wisconsin-Extension
Updated: Sept. 2018

 Homeland Security


ABOUT STOP.THINK.CONNECT.


- In 2009, President Obama issued the *Cyberspace Policy Review*, which tasked the Department of Homeland Security with creating an ongoing cybersecurity awareness campaign – Stop.Think.Connect.™ – to help Americans understand the risks that come with being online.
- Stop.Think.Connect.™** challenges Americans to be more vigilant about practicing safe online habits and encourages them to view Internet safety as a **shared responsibility** at home, in the workplace, and in our communities.

 **UW Extension**
University of Wisconsin-Extension


 Homeland Security

WHY BE CONCERNED?


 **1 IN 3 HOMES**
with computers are infected with **MALICIOUS SOFTWARE**

 **47%**
OF AMERICAN ADULTS have had their personal information exposed by cyber criminals.

600,000
FACEBOOK ACCOUNTS HACKED
every single day.


 **UW Extension**
University of Wisconsin-Extension


Source: Homeland Security (2018)

 Homeland Security

Your Technology Experience


- How do you use the Internet?
- What are your main concerns about using the Internet?
- Have you ever had your identity stolen?
- Do you have antivirus software on your computer and update it on a regular basis?


 **UW Extension**
University of Wisconsin-Extension

 Homeland Security

PASSWORDS


- Change your passwords, at least yearly, every six months is better, and quarterly is great.
- Use a combination of upper and lower case letters, numbers, and special characters.
- Latest research recommends a series of words, separated by one or more special characters:
 - E.g., Adams-Spruce*Lakewood>Eighth
- DON'T** use the same password across all accounts.
- If you must write it down, keep the paper secure.
- Consider using a password manager, if you use a smartphone


 **UW Extension**
University of Wisconsin-Extension


 Homeland Security

TWO-STAGE AUTHENTICATION

- If you have a cellphone, doesn't need to be a smartphone... consider adding two-stage authentication.
- Web service will send you a text with a unique code that will expire when you attempt to log into their site.
- You will need to enter code to complete login.



 **UW Extension**
University of Wisconsin-Extension

 Homeland Security



YOU HAVE ENOUGH TO WORRY ABOUT.
#LockDownURlogin

LOCKDOWNYOURLOGIN.ORG

UW Extension
University of Wisconsin Extension

USING THE INTERNET

- Email, instant messaging, and personal websites provide easy ways for everyone to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances.
- Many scammers target Americans ages 65 and older via emails and websites for charitable donations, online dating services, online auctions, buyer's clubs, health insurance, prescription medications, and health care.
- Many of the crimes that occur in real life – happen on the Internet too. Credit card fraud and identity theft, embezzlement, and more – all can be and are being done online.
- At home, at work, and in the community, our growing use of technology, coupled with increasing cyber threats and risks to our privacy, demands greater security in our online world.

UW Extension
University of Wisconsin Extension

USING PUBLIC/HOTEL WIFI

- Free, unsecure publicly available wi-fi... can help you stay connected to the world, but it can also present incredible security risks.
- Unless absolutely necessary – avoid all banking and financial transactions when using.
- Minimize entry or login credentials.
- When these things must be done, make especially certain that the website is secure.

UW Extension
University of Wisconsin Extension

STOP. THINK. CONNECT. Get savvy about WiFi hotspots. Don't give out personal information, bank or shop over an unsecured network.



STOP | THINK | CONNECT
www.stophinkconnect.org

UW Extension
University of Wisconsin Extension

USING PUBLIC COMPUTERS

- Avoid all online financial transactions.
- Place browser in private browsing mode, if possible.
- When done – erase cache and history from browser.
- Make certain you log out of any accounts (email, etc.)
- You have no control over what is on these devices, and malicious software like keystroke loggers can be installed by other users or employees... website encryption nor VPN's will protect you.
- **If you can, just don't use these devices.**

UW Extension
University of Wisconsin Extension

IDENTITY THEFT



Identity theft is the illegal use of someone else's personal information in order to obtain money or credit.

UW Extension
University of Wisconsin Extension

IDENTITY THEFT



Tips

- **Good password management as we discussed... and don't use the same password and user name for all services.**
- Be careful about answering account/password recovery questions.
 - If your answers can be guessed or researched, someone else might be able to steal your account.
- Do not reveal personally identifiable information online such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or doctor's name.
- Keep your phone and address information up to date for your accounts.




IDENTITY THEFT

- Avoid opening attachments, clicking on links, or responding to email messages from unknown senders or companies that ask for your personal information.
 - Or on computers other than your own
- When making online donations, make sure any charity you donate to is a legitimate non-profit organization and that you type in the web address instead of following a link.
- Be sure to shred bank and credit card statements before throwing them in the trash; talk to your bank about using passwords and photo identification on credit cards and bank accounts.
- **Check your bank and credit card statements monthly for unusual charges.**



LOCATION SHARING

- Be careful about sharing your location:
 - When you travel
 - Of your children or by your children
- On Social media and other web services
- Keep in mind that when you take photos with your cellphone... the phone often automatically embeds *meta data* that includes the GPS location.

PHISHING



***Phishing** is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.*

PHISHING

Tips

- Most organizations – banks, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies.
- Don't access your personal or banking accounts online from a public computer or kiosk.
- Beware of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your passwords often and avoid using the same password for multiple accounts.
- Install and regularly update software firewall, antivirus, and anti-spyware programs.

PHISHING





STOP | THINK | CONNECT
www.stopthinkconnect.org

STOP, THINK, CONNECT. When in doubt, throw it out!
Avoid clicking on suspicious emails, links & social media posts - even if you know the source.

UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

PHARMING

Pharming is a scam that redirects users to false websites without them even knowing it.

Pharming tries to gather user login and personal information.

UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

PHARMING

Tips

- Malicious software can reside on network servers or individual computers... which causes a purposeful misdirection to fake websites.
- Ways to check for pharming:
 - Does the website look different? Good Pharming attempts to closely duplicate a sites appearance.
 - Check for a secure connection.
 - Check the URL, does it look correct.
 - If you typed in login credentials but they didn't work... go back and check the above.
 - If you think you were scammed, go to correct site and change your password now.**

UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

VISHING

Vishing is the telephone version of phishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts.

UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

VISHING

Tips

- People can also use this information to assume your identity and open new bank and credit accounts.
- If you receive an email or phone call requesting you call them and you suspect it might be a fraudulent request, look up the organization's customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Source: Intuit

UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

SMISHING

Smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number.




UW Extension
University of Wisconsin - Extension

STOP THINK CONNECT
Homeland Security

SMISHING

Tips

- The phone number often has an automated voice response system. And again, just like phishing, the smishing message usually asks for your immediate attention.
- In many cases, the smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the text message was sent via email to the cell phone, and not sent from another cell phone.
- Do not respond to smishing messages... legitimate companies do not act in this way.

ONLINE PURCHASES

When Purchasing Online practicing basic consumer safety measures will keep you and your finances safe.










ONLINE PURCHASES

Tips

- Try to stick to one credit card for online purchases, keep track of what you purchase, and audit your bills when they come.
- Never use a debit card online. Debit cards may not carry the same protections that credit cards do. Most credit cards cap consumer loss at \$50, where a bank does not need to offer the same protections with a debit card. Also, debit cards pull money from your account immediately. This money may not be returned until your fraud claim is proven and money returned.
- Know who you are purchasing from.
- Always purchase from secure websites... Look for the certificate or lock in the address bar.

WHEN ARE YOU NOT SECURE

Your Browser Will Provide Clues!










STOP | THINK | CONNECT
www.stopthinkconnect.org

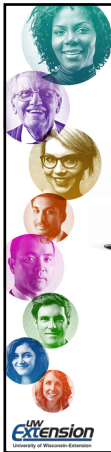


VIRTUAL CREDIT CARD #'s

Tips



- Relatively new product by companies like Citi and Bank of America.
- Assigns a temporary one time or limited use credit card number for one or a set number of transactions.
- If the number is fraudulently obtained, no or limited damage – as the number has either limited spending power, or will automatically expire.
- Virtual credit card numbers will receive a unique expiration date and CVV number as well.











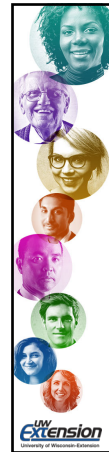
TO SKYPE, OR NOT TO SKYPE

The short answer is, YES! Skype, iMessage, Google Hangouts, etc...








RESOURCES AVAILABLE TO YOU

- **Department of Homeland Security:** <https://www.dhs.gov/topic/cybersecurity>
- **AARP:** The AARP provides specifics on internet safety, how to protect your privacy, and the most up-to-date virus protections.
- **FBI:** This is a list of common fraud schemes aimed at Americans.
- **SeniorNet.org:** SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.
- **Fraud.org:** Fraud.org helps protect consumers from being victimized by fraud.
- **FTC's PassItOn Campaign:** The PassItOn Campaign enlists people 65 and older in an effort to recognize and report fraud and other scams. Topics include imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.



STOP * THINK * CONNECT

For more resources, videos, and training materials... Visit:

www.dhs.gov/stopthinkconnect







Remember...

Stop, think, and then connect when online.



