NATIONAL CYBER SECURITY AWARENESS MONTH: OCTOBER

IT Security is joining a national effort to make the Internet safer.

Keep an eye out for more information on cyber security topics in the UConn Health Lifeline, on displays throughout campus and at an informational event during the month of October.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

October Is National Cybersecurity Awareness Month

Consider these tips for protecting personal information:

- Beware of suspicious emails and phone calls.
- Never enter your user name and password at an unknown or unverified web site.
- Be cautious of websites you visit.
- Think before you click.
- Treat personal information like cash.
- Use strong passwords and never share them.
- Be discreet on social media.
- **Monitor your accounts for suspicious activity.**

IT Security
itsecurity@uchc.edu

UCONN HEALTH

DON'T GET HOOKED!

PHISHING

Phishing is a form of social engineering. Attackers use email or malicious websites to collect personal and financial information.

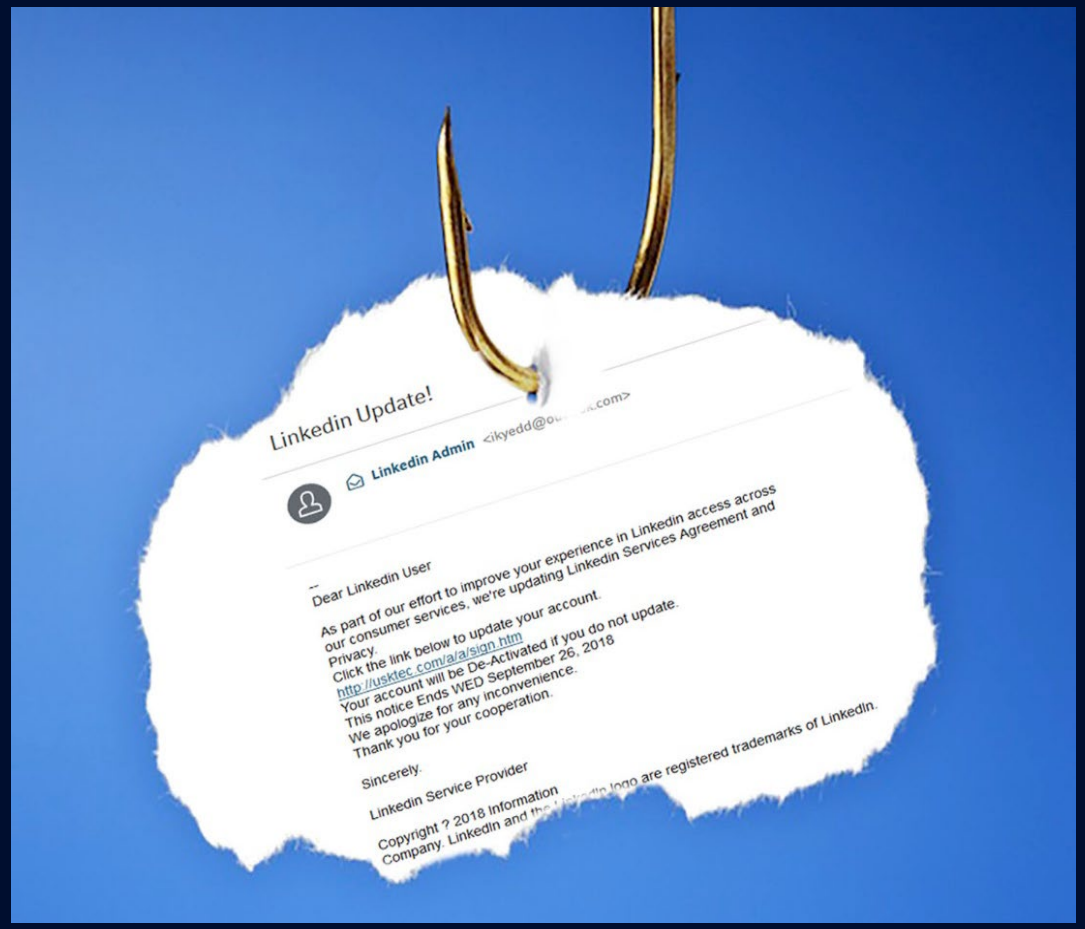
- When in doubt, throw it out.
- Think before you act.
- Delete any request for financial information or passwords.
- Be wary of hyperlinks.

Think you received a phish? Forward it to the Service Desk at servicedesk@uchc.edu.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

I GOT CAUGHT IN A PHISHING SCHEME!



Phishing schemes have become increasingly sophisticated, so don't beat yourself up if you fall for one. If you're the victim of a phishing scheme, here are a few steps to take:

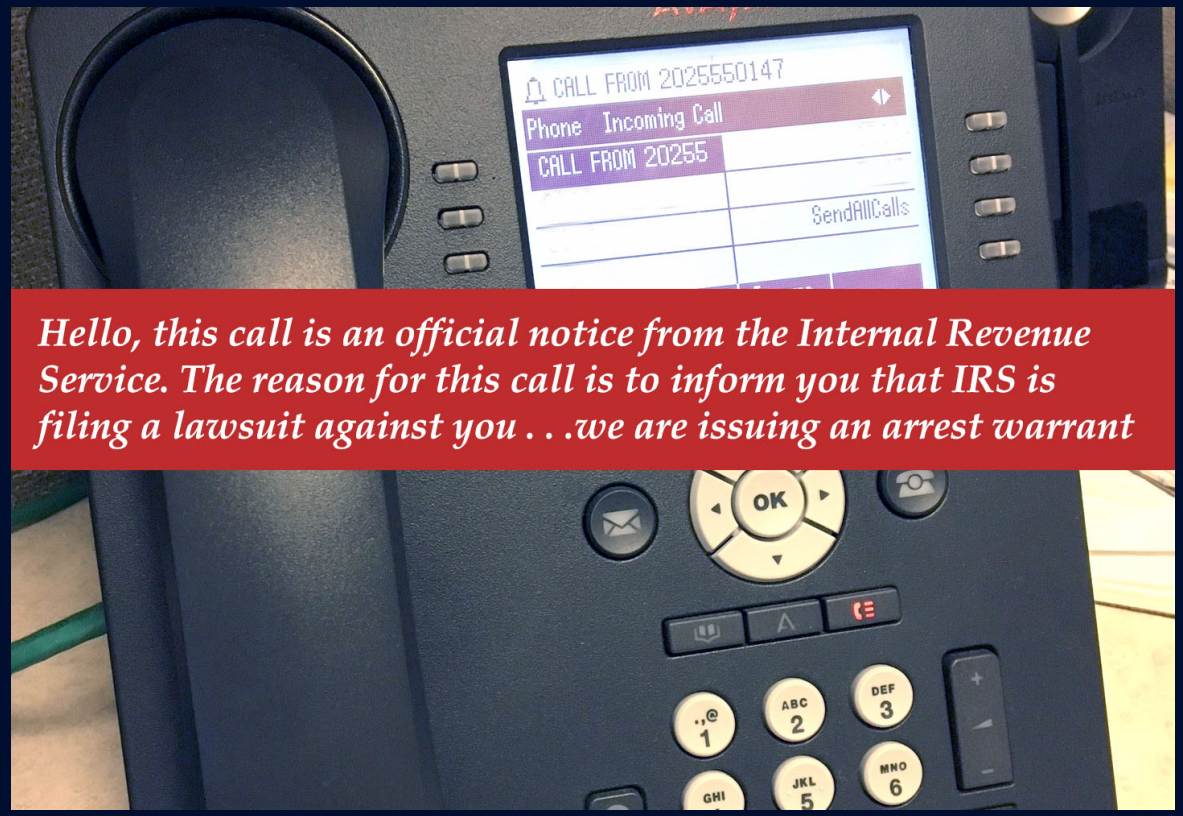
- ✓ Take a deep breath.
- ✓ Change your passwords immediately.
- ✓ Contact the Service Desk at x4400.
- ✓ Forward a copy of the email to servicedesk@uchc.edu.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

BEWARE OF VISHING

Vishing is a form of social engineering that involves contacting victims via telephone and tricking them into giving personal information or money. Attackers will often pose as a legitimate organization, such as a credit card company or a government agency, such as the IRS.



Here are some tips to prevent being a victim of vishing:

- Be suspicious of unknown callers.
- Don't trust caller ID – Attackers can make calls appear to be coming from a legitimate source.
- Ask questions – If someone is asking for your personal information ask them for details about the company.
- Research the company to see if they are legitimate.
- Ask for a number to call the person back or ask to speak to a supervisor.
- Look up contact information for the company and call them directly to confirm the offer.

For more information, contact: IT Service Desk at x4400, Option 2

IT Security
itsecurity@uchc.edu

UCONN HEALTH

SECURE FILE SHARING

Keeping data safe is crucial for protecting confidential data and UConn Health's reputation

One of the biggest threats to the confidentiality of our data is the way files are transferred.

Help protect the confidentiality of our data using the following tips:

- ✓ Avoid sending confidential data via email
- ✓ Avoid transferring data using USB and external hard drive devices. If they must be used make sure that they are encrypted!
- ✓ Use UConn Health's secure file sharing solution

Note that cloud based file sharing services such as DropBox, Google Drive, Apple iCloud, etc. are not authorized for sharing UConn Health's confidential information.

Did you know – Information Technology Services offers a secure file sharing service for transferring and sharing files securely. We can also help you encrypt your USB and external hard drives. Contact the service desk at x4400 for more information.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

DON'T BE FOOLED!

SOCIAL ENGINEERING

Is activity designed to trick people into giving away personal information, and/or installing malicious software onto devices. Attackers do their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

YOUR BEST KEPT SECRET!

PASSWORDS

Passwords are the foundation of information security. Some helpful tips:

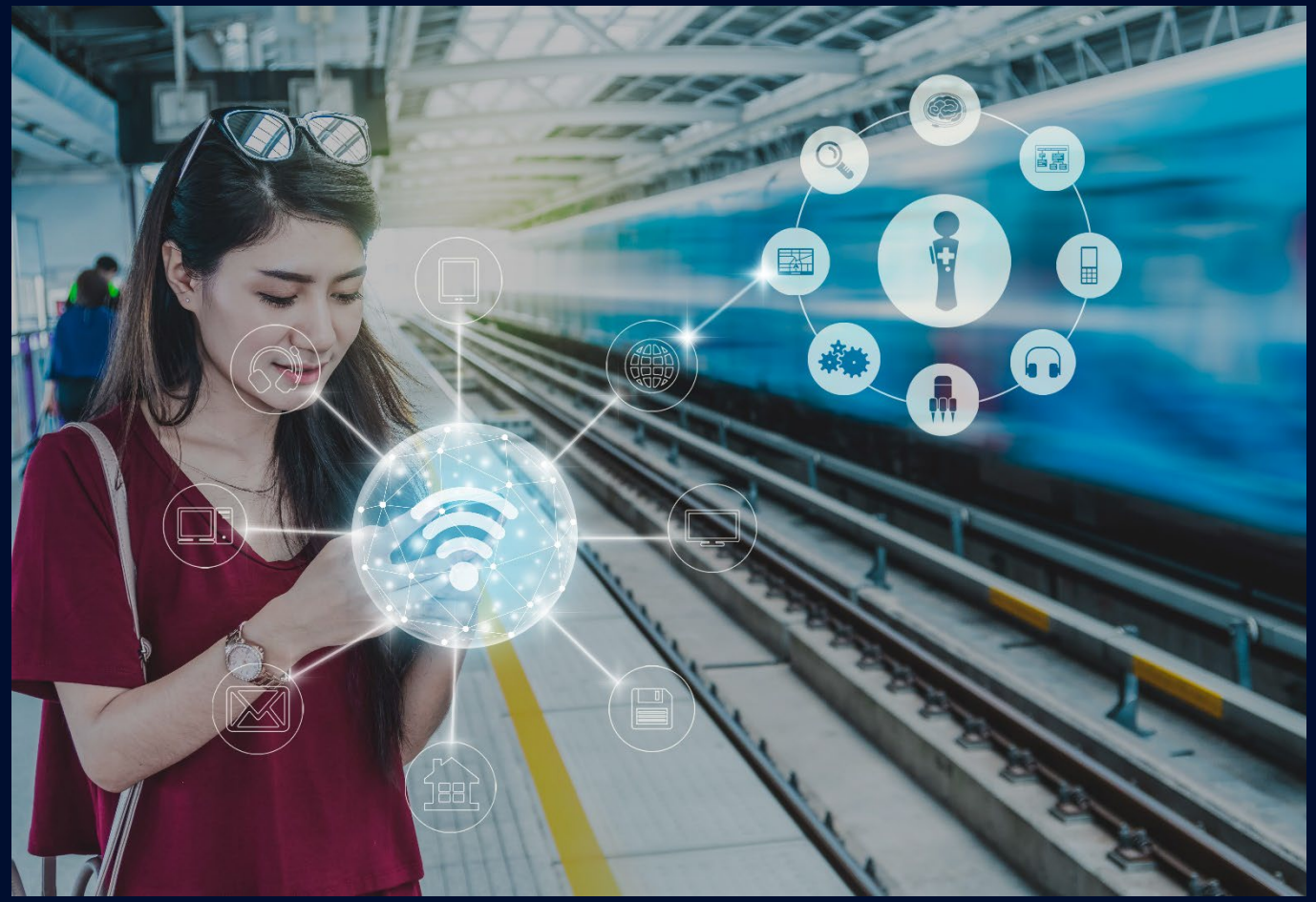
- Create long passwords using letters, numbers and symbols.
- Change them regularly.
- Create passwords from passphrases; they are simple to remember and secure.
- NEVER share your password.
- Use different passwords for different accounts.

If you need assistance with creating or resetting a password, contact the Service Desk at x4400.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

CONNECT SAFELY



Wi-Fi

Wi-Fi networks are everywhere, making it easy for anyone to connect to the Internet wherever they are. Although convenient, they are not always secure. It is important to take measures to protect yourself before connecting to Wi-Fi networks.

- Think before you connect.
- Use your mobile network provider connection.
- Avoid conducting sensitive activities through public networks.
- Keep software up to date.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

DON'T TAKE THE BAIT

SOCIAL MEDIA PHISHING

Social Media Phishing is as the name suggests - Phishing on social media sites like *Facebook* and *LinkedIn*.

- Never click on links in suspicious messages or click on an unverified link, video or file.
- Limit the information available in your profile.
- Don't accept 'friend' requests from people you don't know.
- If you receive an unusual message from someone you know, contact them outside of the social networking site to check their story.
- Spelling errors are telltale signs of a scam.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

DON'T BE A TARGET

MOBILE DEVICE SECURITY

Mobile devices, such as smart phones and tablets, contain as much personal and private information as computers. Here are few tips on keeping personal information on your mobile device secure.

- Use the screen lock.
- Keep software and operating systems up-to-date.
- Only download applications from trusted sources.
- Be aware of applications that track your activity and location.
- Dispose of devices safely by backing up data and then doing a factory reset.

IT Security
itsecurity@uchc.edu

UCONN HEALTH

UConn Health: Acceptable Use Policy

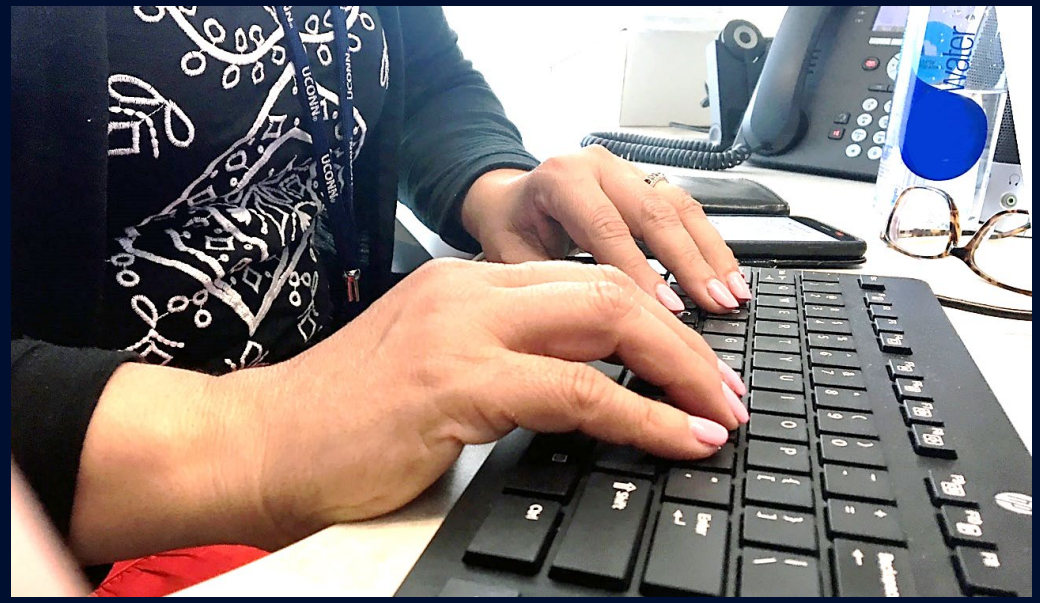
Appropriate use of UConn Health's electronic resources helps to keep our systems, data and patients safe from harm.

Using UConn Health electronic resources (PC's, laptops, phones, network) for personal shopping, checking personal email (Gmail, Yahoo, etc.), watching movies or streaming sporting events and playing games uses critical resources that could affect patient care and exposes our systems to malware and people with malicious intent.

Disabling security controls such as virus protection, login account controls, etc. makes our systems susceptible to compromise.

Help us protect our systems and data by:

- Ensuring that security controls are running at all times.
- Securing data and electronic resources when not in use.
- Protecting mobile devices from theft.
- Report loss or theft to your manager, the UConn Health police or the Information Security Office.



IT Security
itsecurity@uchc.edu

UCONN HEALTH