Mon Health®

Vandalia Health

Information Security
Best Practices for Users

YOU are our first line of defense!

Course Expectations

- To understand what to do – and what not to do - to help protect our computer systems and the information there.
- To be familiar with the tools to help do this.
- To understand that this also means to guard what others might see or hear, whether you're using a computer, phone, or fax – or just conversing with another.

What You Do Matters!

- Systems are secured at the device, system (software and server), *and user* levels.
- Safe practices by IT, software/system vendors, *and users* work together to keep our systems secure from harm.
- As a system user, be mindful of potential information security threats and take steps to avoid them.

Be Aware

- To keep our information secure, each of us must *pay attention to*:
  - What’s on our screens and who else might see it.
  - Who might overhear our conversation.
  - Protect our personally-identified access to computer and phone systems.
  - The email we choose to read and interact with.
  - How we manage printed and faxed materials.

Use Locks & Keys

Physical & System Protections

Who & Where You Are

- Pay attention to your surroundings whenever you login to look at protected information or discuss confidential information on a phone
- Do not leave your device unattended (even in your pocket) without locking your screen or device/workstation.

This protects both you and the one who's information is on the screen or overheard.

Your Username = You

- We log into systems to specifically identify who we are, what we have rights to do, and what we did while there.
- Passwords are your primary way to protect the data in our systems - and your good username - from misuse by others.

About Passwords

- Passwords protect data *and* users.
- You maintain your own passwords to keep them private (usernames are not private).
- Passwords are not to be shared with anyone.
- Online utilities help you manage passwords
  - – Network (ex. Kronos, email, PACS, Nets)
  - – ReadySet

Password Best Practices

- Use different passwords for different systems.
- Use the most complex password you can.*
- Change a password immediately if you think someone else might know it.
- Change it at least every 90 days (often required by our systems).
- Use utilities to help manage your passwords.

Manage Your Passwords

- Register your network password so you can change, unlock, or reset it yourself – *without calling the IT Helpdesk*
- Use similar tools in ReadySet
- Set security questions & answers to secure this service so you can use it when you need to do this yourself.
- Use that system’s password portal

Log Out or **Sign Out** - Do not **X** to close

- Close the systems you've logged into with the provided Log Out or Sign Out links or icons!
- Otherwise, you'll remain logged in and the next user of that device could see and/or do all that you can *under your name*!
- Sign Out/Log Out - *usually* in top right or left corner of the site.

Reboot Your Device - Reset it for next use

- At the end of your shift, reboot your device.
- This resets the memory and settings on the device for the next user.
- This one change in your routine could reduce the number of helpdesk calls you make (and delays in your work) by up to 50%.
- Embrace Windows Updates – they help protect us from security risks

Approved Software & Downloads

- IT Services oversees hardware *and* software licensing and use.
- Software, browser, and Windows conflicts are common, so don’t use other browsers unless directed to by IT.
- Microsoft product lines are our standards.
- Obtain IT approval before downloading *any* software, including trials, or using anything from “the cloud”.

Keep Files on Network Drives

Office users:

- Save your work to one of your user or department folders, NOT a local drive.
- Files on network drives are backed up each day. We’d need these to recover from a ransomware attack or a PC hardware failure.

Flash / Thumb / USB Drives

Use one with caution if you must use it at all

- They can easily be lost or stolen - *Did you set a password on your files?*
- They are notorious for spreading viruses - *Who used it or the PC before you? Trustworthy?*
- ***DO NOT*** *– Store Protected information on these devices*

Bring it to IT to safely scan the files before you access any files on a USB drive given to you.

Physical protections – Paper & more

- Patient, employee, and other confidential data may be on CDs and other media – even paper - as part of the work process.
- Never leave confidential information sitting out unattended.
- Fax machines and printers should never be in public areas but pick up printouts as quickly as possible anyway.

Faxes / Email – Responsibilities

- Use Mon Health approved Fax Cover Sheets – find on intranet via site search.
- Confidentiality wording for misdirected ones.
- Sending: double-check you’re sending to the right person, department, and number.
- Receiving: if not for you, contact the sender to resend and maybe correct their contact list.
- Both - work to redirect or resend message

Properly Dispose Of Confidential Material

- When no longer useful or usable: shred paper and thin computer media.
- Shred bins are available in most every area for paper, CDs, DVDs, and memory cards.
- Computer or communication equipment must go to IT to destroy.
- Refer to Disposal of Confidential Materials policy for more information.

Don’t Get Tangled in the Web

Web Use Best Practices

- Use Microsoft Edge for higher security, and don’t change settings without an IT OK.
- Use links on our Intranet whenever possible – they’ve been approved and recommended by Mon Health staff.
- The Intranet should be the default homepage for all PCs.

Web Search Best Practices

- If you must search the web, **Google is the big search engine that should** be used. It’s the only one that considers site *content* to help with result rankings.
- Call IT if Google isn’t your default search engine.

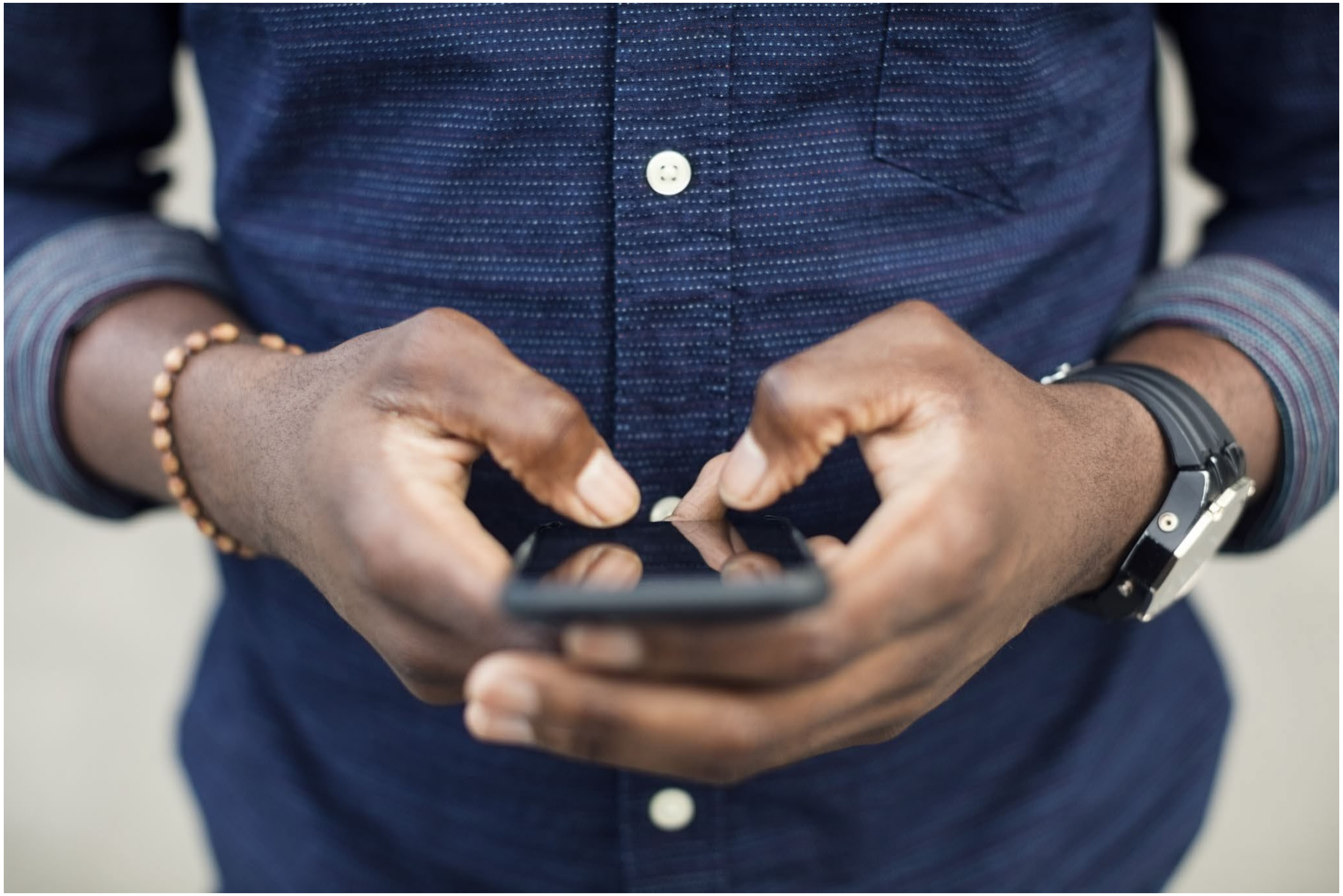
Web Search *Result* Best Practices

- Look past links with Ad in front of them. The high rankings have been bought, rather than earned. It's wiser to use valid search results.
- Try to stay within the first few pages of results, as others may be less reliable (certainly less often referenced).
- Search another term if you don't find what you need.

Personal Web Use

- Our corporate standards apply to this use.
- Do not (attempt to) go to websites you wouldn’t want your boss or the IT Security Officer to know about.

Personal Devices



- Per our Bring Your Own Device policy, personal devices are permitted in the organization.
- Organizational or departmental policies may apply to the use of personal devices.
- You may NOT connect personal devices to internal networks.
- You may NOT use cameras to capture photos or videos of data that may contain protected information.

Email

Best Friend, Worst Enemy

Email Best Practices

Email is the most common way to spread ransomware and other computer viruses to user devices and then through an entire organization.

This puts you in the driver’s seat.

Why Is Email Such A Target?

- Email is the one system that most frequently connects us to other users – both inside and outside our network and organization.
- We tend to trust that other people share our values.
- We’re busy and often do not stop to question whether each email message, with links or attachments, is expected or not.

Treat Every Email As A Threat

- Expected communication?
- Expected attachment or hyperlink?

Do This

- Hover over any URL before you select it and look for an expected URL for that company.
- Call or send a fresh email to your contact, go to your browser and Google the company, or type in a known website to look for the info.

Don’t Fall For Scare Tactics

- **No** reputable company, agency, or even a hospital department – especially IT - would ever send an **email** to verify your username, password, or other personal information.
- No one should ask you to click a link to avoid legal action or keep access to anything.
- No matter who the sender *appears* to be, especially if it’s “from you”, STOP to Think!

What should I do if I receive a suspicious email?

- Use “Report Phish” tools contained within your email applications.
- Do Not forward the email to co-workers and ask them to review.
- Do Not respond to the sender asking for additional information.

Is that email valid?

When in doubt, delete it!

Unless….

If It’s Ransomware….

1. If the email you just opened says that your files are encrypted, and you can get them back when you pay money (or bitcoin).

2. **Turn off your device!**
   Just hit the power button (or pull the plug or battery).

3. **Take a breath and call the IT Helpdesk.**

You’re the Driver

Let’s Review…

- Pay Attention to your surroundings and what’s on your screen and what you say
- Protect your devices, your files, your passwords
- Use approved software and best practices
- Think – is this expected or out of the ordinary?

When You Have Questions

- Site Search on our Intranet for how-to information
- Call the IT Helpdesk at 304-598-1327
  - IT logs calls for requests for assistance.
  - Calls are directed to the right team (member) to help you most quickly.

Thank You!