



MANKATO

COMPUTER TECHNOLOGY

Professional Business Solutions

Computer Safety



Common Mistakes when it comes to protecting your Computer

➤ Physically

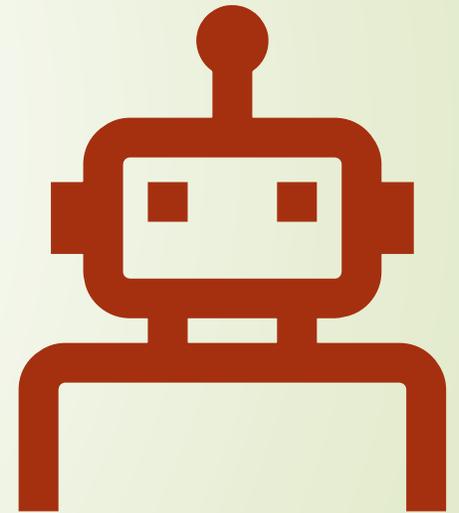
- Having strong passwords but leaving your computer unlocked in public places

➤ Technically

- Having good anti virus software but replying to or forwarding suspicious email

What we want to do today:

- ▶ Help Build Confidence when it comes to using your computer
- ▶ Give you a list of suggestions and tips
 - ▶ You can try them yourself or schedule a time for us to come help you
 - ▶ This list was created from a similar list that they give to the Incoming students at MIT
 - ▶ Everyone can always use to learn new tips or just have a refresher or reminder
 - ▶ Create a friendly environment for you to operate your computer at a higher level and on a safer basis
 - ▶ Special thanks to Mankato Computer Repair for making this possible.



Tip #1 Keep your computer up to date

- Spend time doing software and operating system updates
- Turn on Automatic updates
- Having the latest version may not seem the most convenient, but usually will help keep you the safest.
- There is always a learning curve when changes happen to your favorite programs but overall they are designed to keep your experience safe
- When in doubt do some research, or ask questions

Tip #2 Install Protective Software



It's unlikely you'll get hit with an actual computer virus.



Malware these days is about making money, and there's no easy way to cash in on spreading a virus.



Ransomware and data-stealing Trojans are much more common, as are bots that let the bot-herder rent out your computer for nefarious purposes.



Modern antivirus utilities handle Trojans, rootkits, spyware, adware, ransomware, and more.



Some Suggestions

- ▶ Vipre Antivirus is recommended
 - ▶ protects against viruses and spyware as well as threats from email, instant messaging and removable media
 - ▶ full-featured entry-level protection that effectively detects and blocks prevalent malware
- ▶ Webroot Antivirus is part of the Premier care support program at Mankato Computer Repair
- ▶ Windows Defender is a software product that attempts to detect and remove malware. Initially released as an antispymware program, it was first released as a free download for **Windows** XP, shipped with **Windows** Vista and by default, and currently ships with antivirus capabilities as part of **Windows** 10.

Tip #3 Create Strong Passwords

- Password selection should include
 - Letters, Numbers and Special Characters
 - It should be easy to remember
 - Try to change them regularly, even if they are on a rotation
- Some Longer passwords are so simple their extra length is worthless
- Many people try to be more secure by adding characters to passwords but if these longer passwords are based on simple patterns they will put you in just as much risk as having your identity stolen by hackers
- There are programs such as last pass that will help manage passwords for you.

PASSWORDS are like UNDERWEAR

1. Change them regularly
2. Don't leave them on your desk
3. Don't loan them to anyone





Worst Passwords of 2015

1234, 12345, 123456, 1234567, 12345678, 123456789

Password

Qwerty

Football

Baseball

Welcome

Abc123

111111

1qaz2wsx

Dragon

Master

Monkey

Letmein

Tip #4 BACKUP BACKUP BACKUP

- External hard drives
- Acronis True image
- Nightly Backups
- Live Drive (carbonite) \$60 a year unlimited storage
 - Included in the \$99 Premier care support program
- Backup Hard drive
- Router/USB options
- One Drive
- iCloud

Tip #5
Control
Access to
your
Machine(s)



Separate logins for individual users



General Placement in Public locations



Physical Security is as important as technical security



Secure Disposal



Lock your computer, lock the screen with a password



Tip #6 Use the internet and email safely

- ▶ We live in an age of connection, we have the tools to build trust, remember what things were like before caller id and we had to answer the phone, now we require trust before we take a call from a telemarketer.
- ▶ We need to learn this safety practice with computers as well.
- ▶ Set email filters, junk mail, rules
- ▶ Have a strict safe contact list
- ▶ Be wary of links and attachments in emails as well as popups and advertisements on web pages (alt F4 instead of closing with the X)
- ▶ Don't trust unsolicited calls about your computer, and never give remote access to someone you don't know or trust

Suggestions



Create multiple email accounts for various activities, Email, Shopping, Work, Contests, Bills, Memberships.



Only Respond to email addresses you recognize, check the email address not just the sender's name



When in doubt talk to someone you trust about it.



It's actually incredibly polite to let someone know they've been hacked.



You can use google to look up phone numbers to see who just called you



Scan attachments, validate links, reduce your risk for identity theft



Look for the (S) in http://

Email tips

- ▶ Everything on an email can be made public to be careful what you send
- ▶ Look out for subject lines in all caps, all in lower case and those that include URL's and exclamation points.
- ▶ Make sure the subject line matches the message
- ▶ Make sure the sender matches the signature
- ▶ Avoid attachments from unknown senders
- ▶ Pick up the phone if you are unsure
- ▶ Evaluate the importance of the email
- ▶ No Matter what you haven't won the lottery from a Nigerian prince, and no one from Microsoft will call you to ask for access to your computer.
- ▶ You can use Snopes.com to look out for scams, just type in the first few words of the email.



It's a SCAM

- ▶ Does somebody want to transfer millions of dollars into your account?
- ▶ Does someone want to pay you to cash checks and send them the money?
- ▶ Met a new friend/pen pal on a friendship/dating site who's asking you for money?
- ▶ Has a dying person contacted you wanting your help to give his money to charity?
- ▶ Have you sold an item and are asked to accept a payment larger than the item amount?
- ▶ unclaimed insurance bonds, diamond-encrusted safe deposit boxes, close friends marooned in a foreign country.

How Bad is the Problem?

- **2.1 Million Fraud Reports from Consumers in 2020**
 - 1/3 Lost Money
 - 33% Aged 20-29
- **\$3.3 Billion Lost to Fraud in 2020**
 - Over 80% increase from 2019
 - Pandemic was fuel on the fire

Source: [FTC](#)



Where do Scams Come From?

➤ Email

- 94% of attacks originate in email
- Impersonation attacks
- Phishing/Whale Phishing
- Malware/Viruses/Ransomware

➤ Phone Calls

- “Vishing”
- Impersonation
- Tech Support Scams



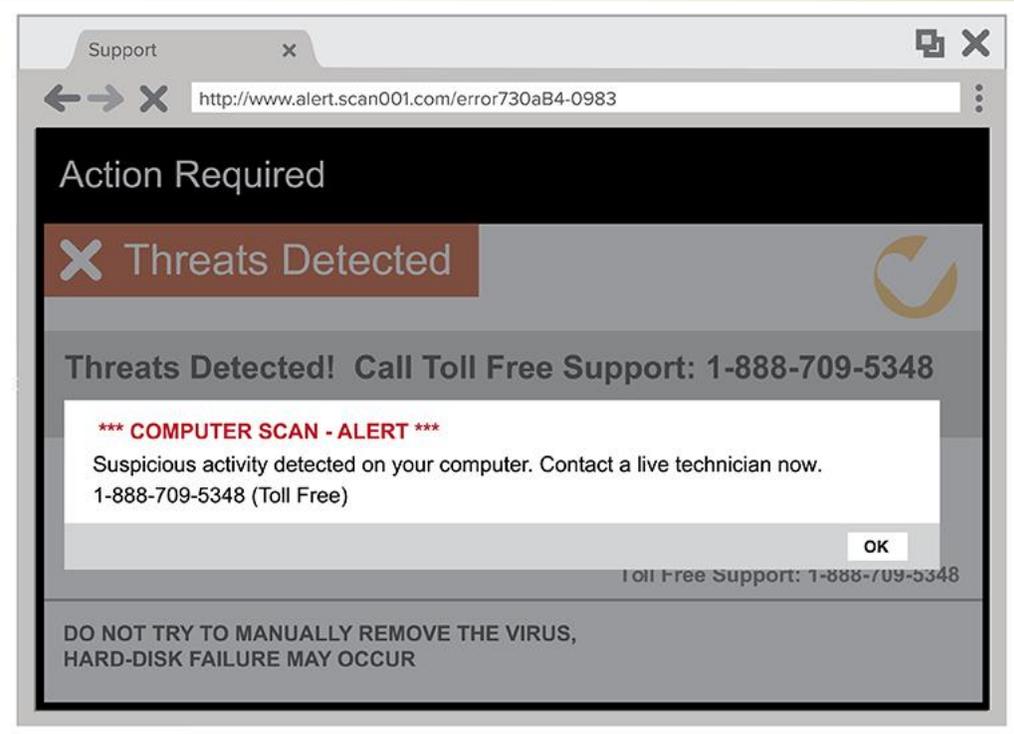
Where do Scams Come From? (cont.)

➤ Pop Up Ads

- Fake search results
- Advertisements on web pages
- Pop up messages

➤ Major Breaches

- Yahoo (Aug 2013)
- LinkedIn (June 2021)
- Facebook (April 2019)



Common Local Scams

➤ **“Vishing” AKA Phone Scams**

- IRS Scam
- Jail Scam
- Computer/Virus Scams

➤ **Impersonation Attacks**

- Trusted Figures – Pastors & Bosses
- Payroll Scams
- Gift card Scams
- Verizon Scam
- Real Estate/Title Scams



Common Local Scams (cont.)

➤ **Blackmail Emails**

- Webcam Bluff Scam

➤ **Phishing**

- Compromised Email Accounts
- Hacks are Monetized Quickly

➤ **Computer Pop Ups & Ads**

- Fake Security Programs
- Fake Messages from Security Companies
- Browser Hijacking



What Can Be Done?

- **Err on the side of caution**
 - Never trust anyone contacting you
 - Pause before giving out personal info
 - Pick up the phone
- **Look for red flags**
 - Spelling/grammar
 - Sender domain
 - Links – hover mouse
- **Serious Limitations – the bad guys are too good**



What would it be like to Spam them back?

- ▶ They pop up in our inboxes, and standard procedure is to delete on sight. But what happens when you reply? Follow along as writer and comedian James Veitch narrates a hilarious, weeks-long exchange with a spammer who offered to cut him in on a hot deal.
- ▶ https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email?language=en



Tip #7 Just because it's free Wi-Fi doesn't mean it's a good idea to log into it.

- Don't have your automatic settings to log in to any available network
- Make sure your device asks you before connecting to it
- Use secure connections and VPN's when possible
- If you must use a public network, log off as soon as you are done using it.
- While on a public network please avoid using your bank website, secure information, or anything you wouldn't want someone else to see.



Tip #8
Protect
sensitive data



Remove sensitive files from your hard drive especially if you are recycling or repurposing your computer



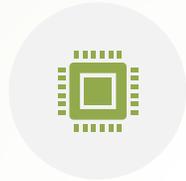
Clear your browsing history, delete junk mail, and trash



Keep in mind, nothing is ever truly deleted 😞



Tip #9 Firewalls



A Firewall is a part of a computer system or network that is designed to block unauthorized access while permitting outward communication.



MAC and Windows computers come with them, learn how to set them up and use them



Make sure it is turned on

Preventative Measures

- **MFA for everything!**
 - Email, banks, and social media in particular
- **Email Security**
 - Secure Passwords, spam filter, MFA
- **Antivirus**
 - Don't use free, keep it up to date
- **Update, update, update**
 - Windows Patches
 - 3rd party patches



Tip #10 Stay informed and other quick tips

- Talk to Experts, Visit trusted Websites, Read Blogs, Come into MCR
- Download files Legally
- Limit information on Social Media sites, and chose applications carefully
- Avoid surfing websites you don't know
- Don't install software you don't need
- Avoid keeping magnets and liquids near your computer
- When transporting your computer shut it down or make sure it is hibernating
- Keep it well ventilated and clean.
- Keep close track of your financial info if you are online at all.

Email Security



Avoid clicking links which look like gibberish, are sent to you by unknown persons or that seem unusual for the person who sent it.



Be wary of attachments as they are a popular venue for viruses. Look for common file extensions like .docx, .pptx, .pdf, and .jpg. Even so, be careful—some viruses masquerade as images! Avoid .exe or .com files unless you trust the person intended to send you one of those.



Set your anti-virus suite to scan incoming emails and downloaded attachments.



Check the “full headers” of an email message to determine the true source of it (look for the Return-Path field). Be wary of emails where Return-Path and from differ.



Be wary of emails asking for your log in information, especially if they appear to come from some “system administrator” or “IT team” or “security team.” Make sure the email address contains the correct domain (uoregon.edu for example) and check with MCR if you think it still sounds fishy.

Preventative Measures (cont.)

- **Air gapped backup**
 - Backup with versioning & air-gapped is best answer to ransomware
- **Secure Passwords**
 - 10 characters or more
 - Complexity requirements
 - Change every 6 months
 - Don't use same password everywhere
- **In a business setting, work with the pros**



Web and Social networking security



Use common sense. A trustworthy website will be well-organized, appear official and will help you find information or perform an action.



When deciding whether to click a link, hover your mouse over the link. Check the bottom bar of the program you are in, or wait for a little box to pop up over the cursor. If the link in one of these places differs from the link that was linked to you, don't click it!



Avoid using excessive Facebook applications. Many applications are fronts for viruses or account hijackers.



Close suspicious windows and pop-up ads by using Alt-F4 rather than the X button.



Watch out for redirects. If you click on one link and end up on some other page, especially if it looks shady, the page may be dangerous or you may have a browser hijacker.



Use ad blockers, JavaScript blockers and Flash blockers. Ask for help choosing JavaScript or Flash blockers, since many legitimate applications and tools use these things (such as YouTube).

Closing Thoughts

- **Most scams just involve tricking people**
 - Not technically sophisticated
- **Trust your gut**
- **Listen to the experts**
- **Stay educated on latest threats**





Top Ten Tips

- 1. Keep your computer up to date
- 2. Install Protective software
- 3. Create Strong Passwords
- 4. Backup and Save
- 5. Control access to your machines
- 6. Use the internet and email safely
- 7. Be Wary of Free Wi-Fi
- 8. Protect Sensitive Data
- 9. Firewalls
- 10. Stay Informed (practice, practice, practice)