IT Annual Security Bulletin

October is National Cyber Security Awareness Month!

Online Scams: Watch Out for These Common Red Flags

Scams aren't new -- they've been around for as long as humanity has existed. They are used to deceive unsuspecting people in order to gain information, money, or influence. With the rise of the Internet, scams have become more prevalent. Scammers send out millions of email scams every day in order to cast a world-wide net. A list of the current top 11 online scams is shown below. If you're aware of these scams, you're a lot less likely to fall for them.

Phishing is by far the most common, and potentially the most dangerous, scam. A common phishing technique involves getting a target to log into a fake site or fill out a form with their account (e.g., bank, social media, credit card, etc.) login information. This is often done via a faked/spoofed email. It may look like you have logged in or submitted a form, but you have actually given your user name and password (or other personal information) to cybercriminals. It's important to know how to identify phishing attempts to avoid getting hooked.

Fake antivirus software has become a common way for scammers to slip Trojan horses and other malicious software into people's computers in order to steal account credentials (login information) and/or personal information. Some malicious code can even be used to take control of the infected computer.

Text message scams are another type of phishing attack. They can be made to look like they came from anyone (Apple, your bank, or a service like PayPal). If you receive a text from a company or group, don't call the phone number or click on the link that may be provided. Instead, go to the company's website and find their official number or contact.

Inside this Issue:

Online Scams: Watch Out for These Common Red Flags Continued...

Fake software updates are multiplying these days. Many of them masquerade as Adobe Flash Player installers or Microsoft Office updates. As with fake antivirus software, these software updates can compromise your computer and enable cybercriminals to access all your data.

Facebook question and answer scams may appear innocent at first. Sometimes on Facebook, people may randomly ask questions like: *"What was your first car? Who was your best friend as a child?"* If you've seen Apple's security questions, you'll notice that these are the same. Don't ever answer these questions. If scammers can get one or two answers like this, they can get into your account by resetting your password.

Typosquatting is a relatively new phenomenon. This scam takes advantage of mistyped URLs by purposely creating malicious websites with slightly misspelled domain name endings (.om or .cm instead of .com) and domain names (amozon.com instead of amazon.com). We all make typing mistakes, so it's important to be very careful when we enter a URL.

Online tax filing scams flourish at certain times of the year. They take advantage of the fact that many people pay their taxes at the last minute and are perhaps stressed at having to pay out what may be a large sum of money. Make sure that you're at the right website and not some typosquatter site when you file and/or pay your taxes. If you use an app to file your taxes, make sure it's up to date. If you can, try to file your taxes early when you are not in a hurry. This way, you can better spot the signs of a bogus website or app.

Free Wi-Fi scams are increasingly common, as we all need to use wi-fi when we're not at home or at the office. Use these tips to make sure your mobile device is safe on public networks. Remove Wi-Fi networks you no longer connect to from your device, and use a VPN to stay secure.

Online shopping scams are another way to separate you from your money. They are very common around the holiday period. Sometimes you'll encounter fake websites, and other times people may try to offer to sell you something directly (rather than on eBay or Amazon), so you can "save money." Remember that these big e-commerce sites generally guarantee your transactions, so don't try to shave a bit of money off your purchase and end up with nothing.

Stay Safe Online!

StaySafeOnline offers both business and family oriented-educational tips and guides for using the Internet safely. For users with all levels of computer experience, this is a great informative platform that is updated on a regular basis.

IT Security Quick Links

The IT Security webpage has a tech tip section, a tech terms cheat sheet for tech jargon, and offers easy access to all IT related policies for CTC.

Online Scams: Watch Out for These Common Red Flags Continued...

Online dating scams may start as a text or email that reads like this: “*Dear ___, My name is Ann, and finally I decided to write to you. I’m from Russia, but now I live in the USA. I saw your photos on Facebook and can’t get you out from my head. You look cute and at the same time very sexy and smart, just like my type. Wanna talk to you, what about you?*” But not all online dating scams are that blatant; some can be very subtle. Be aware that scammers will work to exploit your heart if given the chance.

Fake news and articles have really started to increase in number lately. While in some contexts the term fake news can refer to journalism with a political bias, there are also literal fake news sites that impersonate real news sources. These fake news sites are often used in conjunction with spam to either deceptively advertise products or to try to convince victims to fall for scams.

IT Security Quick Links

If you’re looking for an encryption tool, the IT Division recommends Encryption Wizard. A guide can be found on the IT Security Tech Tip page.

How Else Can I Stay Protected?

Using the checklist below, learn how to quickly identify potential email phishing scams. If you answer yes to any of the following questions, the email you just opened may be a scam.

- Is the email from someone you do not know personally or communicate with normally?
- Is the sender’s email address from a suspicious sounding domain? (*example: @micro-softsupport.com, @paypal-security.net*)
- Were you CC’ed on an email with some other people you do not know?
- Does the subject line seem irrelevant, not make sense, or not match the content of the email?
- Is the email a reply to a message you never sent?
- Did the email come at an odd time, like 2:00 am?
- Is the sender asking you to click on a link or open an attachment?
- Does the email contain an .htm, a .zip, or other executable file?
- When you hover over any links within the email, does it show a different link than what is contained within the body of the email?
- Does the email contain a link, but no other information?

How Else Can I Stay Protected Continued...

- Is the link to a well-known website, but spelled incorrectly and somewhat suspicious looking? (*example: paypal.paymentsnow.com, bankofamericacom.net*)
- Is the sender stating something bad will happen if you do not click the link, or that there is extreme value in clicking the link?
- Does the email contain poor grammar or spelling mistakes?
- Is the sender warning you that they found inappropriate content or images of you online?
- Does something just seem off?
- If you feel the email is a phishing attempt, notify the IT Division immediately.

If you think the email is **legitimate**, but you're still concerned, then follow these steps:

- Do a Google search for the company name that the email has come from.
- Visit their website and look for a phone number or email address.
- Call or email the business and ask them to verify the information within the email.
- If you know the sender, call the person and confirm they sent the email.

Of course, cybercriminals are always trying to find new ways to deceive, attack, or infect their victims. That's why it's important to stay up-to-date on all the latest developments in online safety.

You can read both of these articles and find other great security articles here:

- ♦ Top 10 online scams: Watch out for these common red flags
  Kirk McElhearn, intego - The Mac Security Blog
- ♦ How to Identify an Email Scam in 10 Seconds or Less
  Netcetera

Tell the IT Help Desk!

If you think you have become the victim of a ransomware or malware, please contact the IT Division immediately. The sooner we can address the situation, the better the chance we have at recovering your data.

Ask The Help Desk

You can report phishing emails to the IT Help Desk, or ask the IT Help Desk to verify emails that you are not sure about.

The New Password Policy & Why You Need a Password Manager

Passwords play a central role in maintaining security. On July 5, 2022, CTC's password policy was changed to match newly improved security standards. These new standards state that a longer, more difficult password to guess is stronger than a password that is constantly changed on a schedule.

And while it is good to have a strong password that never expires, it can be difficult to remember a password that is 16 or more characters long and made up of a mix of uppercase letters, lowercase letters, and numbers. Likewise, entering it correctly into multiple applications that are needed for everyday work can be both frustrating and tedious.

"Password mangers are a fantastic way to both keep your login information safe and to save time."

This is where a password manager can really come in handy. A password manager is an application that can be used to store your login information. Many password mangers also come with a password generator, which can be used to make strong passwords for you. Information stored in a password manager is often encrypted and locked behind a password. (This means, you will only have to remember one password for logging into your computer, and one password to access all your stored passwords on your password manger.) Password mangers are a fantastic way to both keep your login information safe and to save time.

Two commonly used types of password mangers include desktop-based password managers and cloud-based password managers. Desktop-based password managers can only be accessed on the computer they are downloaded onto. Likewise, information stored in these types of managers is kept on your computer. This is great for security, but keeping a backup (on a flash drive or shared drive) is recommended. Otherwise, you risk losing all your password information should your hard drive crash.

Review HR Policies 294 & 295

Remember to review:

- HR Policy 294 on Computer Security &
- HR Policy 295 on Computer Usage.

It's Time to Have the Tech Talk

Don't forget to talk to your family about saying safe online! If you need help starting the conversation or keeping track of what to cover, the IT Division recommends Mozilla Firefox's The TechTalk.

The New Password Policy & Why You Need a Password Manager Continued...

On the other end, cloud-based managers can be accessed through multiple devices (usually via an app or browser). This is convenient, but this also means storing your login and password information on another business or company's server. While most cloud-based password mangers are secure, there is always the chance that your cloud-based manager of choice might be targeted and breached.

The IT Division recommends KeePass for anyone looking for a new password manager. KeePass is a free and open source, desktop-based password manger that also comes with its own password generator. You can download KeePass from https://keepass.info/.

> *"A password that might take weeks to decipher is less appealing than one that might take only five minutes."*

Remember!!!

- The IT Division/IT Help Desk will **NEVER** ask for your login information!
- We will **NEVER** email you about changing your password.
- Updates/software fixes will **NEVER** be sent through email!

Create Strong Passwords & Store Them in Your Password Manger

Now that you have a password manger, it's time to put it to good use. But what makes a strong, secure password? Here are some tips:

- Don't use the same password over and over. You only need to remember the passwords for your desktop computer and your manager, so make all your other passwords for sites and accounts unique. Should one password ever be cracked or stolen, it will only affect the one account it is used for.

- Longer passwords are always better. The longer the password, the longer it will take for a human or computer to crack it. A password that might take weeks to decipher is less appealing than one that might take only five minutes. Passwords should be at least 12 characters in length, though many security organizations recommend a 16-character minimum — a standard which CTC has adopted.

Create Strong Passwords & Store Them in Your Password Manger Continued…

- Use a passphrase. A great way to throw together a secure password is to combine four random words together. Items in your office, car, or building may give you ideas, such as “lamp blue staple light” or “hall plant orange calendar.” Avoid common phrases, as phrases are checked against in many cracking applications.

- Make your passwords complex. Passwords should be made up of a mix of upper and lowercase letters, numbers, and special characters (example: @, $, %, &) when the option is available. (Example: “lamp blue staple light” would become “l@Mp b1U3 $T4p13-lIgH7”)

- Take advantage of your password manager’s password generator. You can tell most generators to include all the tips listed above when generating a new password. This is especially

CTC IT Division

The IT Help Desk is the first point of contact for computing and telephone services offered by the CTC IT Division. We are located in the Administrative Computer Center (*building 551*).

The CTC IT Help Desk is OPEN
Monday – Thursday: 7:00 a.m. to 5:30 p.m. CST
Friday: 7:00 a.m. to 11:30 a.m. CST

Call the IT Help Desk
Local: 254-501-3103
In-State: 800-223-4760 Ext 3103
Out-of-State: 800-792-3348 Ext 3103

Email the IT Help Desk
help.desk@ctcd.edu