Common Tech-Related Scams

# EMAIL

**Gift card scam**

You are asked to buy gift cards, often from someone impersonating a figure of authority. These are researched and personal to you, for example your boss or someone higher in the organization. These come up with a cover story, asking you to buy gift cards and take photo of codes, sending it to them and promising to repay quickly. These scam messages could be SMS “text message” or email. If you are ever asked over an electronic communication to buy or pay with gift cards, it is probably a scam.

**Photo/Video Extortion**

One common extortion message is scripted like this: They claim to have hacked your account and/or device. They try provide “proof” to convince you, such as listing a previously leaked password from an external services you may have signed up for with your email address, or they spoof a message to look it like was sent from your account. They then ask you to pay in cryptocurrency, such as bitcoin, so that they delete embarrassing videos “they took of you with your webcam” instead of publishing them to your friends and coworkers. In reality, they have no such video and did not hack you in any way. They are hoping you will just pay. You can safely delete these.

**Fake purchase of service/products**

You may receive an email notification for a product or service you did not buy. Often these emails have only a phone number to call and no web links, and recently use a theme of an automatic “Geek Squad” service renewal has been extremely common. If you call, they will ask you for information as well as asking you to connect from your computer to a remote support service where they can see and control your computer. This can lead to malware, identity theft, and fraudulent charges. It would seem uncommon for any business that has online transactions and yet only has a phone number to call with no email links. Online businesses typically prefer you to solve your own problems instead of calling them. You can safely delete these.

**Business Email Compromise**

Scammers will impersonate employees and vendors, attempting to get bank deposit information changed for billing and payroll.  Ensure that process requires to verify with the person via known, previously provided contact information before changing bank info.

Scammers will setup lookalike domains and email address to impersonate others as well.  If the real vendor contact was validcontact@vendor.**com**, the attacker used validcontact@vendor.**net** and asked for the payments to be sent to the new bank.  It would be difficult to notice the tiny difference - only a strong process like this will ensure these scams can be reliably caught.

**Thread Hijacking**

Scammers will use an existing email chain that they managed to obtain and insert themselves into the conversation, injecting malicious attachments, links, or asking for harmful changes, such as new banking information. This tactic is designed to trick you let into your guard down by showing you something familiar.

**Grand Piano Giveaway**

Scammers claim to be giving away expensive name-brand pianos. If you agree to accept it, the scammer will ask you for money to cover the moving costs from a location out of your area. They will keep the money and give you nothing in return.

# SMS – Text Message

Most email phishing tactics also apply to SMS text messages and other messaging apps you might use. However, mobile usage complicates things in some additional ways:

* You might know a person’s email, but not their cell phone number. If a text message you receive claims to be someone you know, you might be more likely to believe it than an email. Be wary of messages from unknown numbers, regardless of who the sender claims to be. If you did not provide your phone number to that individual and receive a text from an unrecognized phone number claiming to be them, chances are the sender is not who they claim.
* Your phone will be less protected than your work systems. Your phone and the cellular networks are not tied into work and cannot filter, monitor, or protect your device, network connections, text messages, or other messaging apps.
* Scammers will research and impersonate people you know and work with, often impersonating positions of authority. Using SMS has the advantage or operating outside of email system protections and may be more likely to catch you off guard.

# QR Codes

QR codes are those blocky barcode-like images that direct your device to a web location. They are nothing more than links to a website with the main exception being you generally have no idea where it will lead you to. This makes it very convenient for attackers to trick you into going to a malicious website without having the benefit of web filtering that a Tri-C managed computer would have.

**QR Codes in Email**

Sending QR codes via email is a way to bypass email filtering as typically email protections do not have the ability to effectively examine QR codes. It also benefits the attacker by moving the attack to a mobile phone which usually has less protection and is more difficult to see the full website. There is NO REASON a QR code should be in an email! Since a QR code only functions as a link, using a regular clickable link is both more convenient and easier to determine where it leads. Always assume a QR code in email is phishing!

**QR Code Replacement**

This technique involves placing a replacement QR code sticker over a business’s legitimate QR code. The replacement QR codes leads to a malicious website that will attempt to phish you or install malware on your device.

**QR Code Tips**

* Cyberattacks are designed to catch you off guard and trigger you to scan impulsively. Does a QR code make sense in the context in which you are using it? Is it somewhere you would only expect a mobile device to be used?
* When possible, navigate to a website instead of using QR codes.
* Typically, when you scan a QR code, you can see a small part of the destination website. Ensure it matches where you are expecting to navigate to.

Be cautious before entering any sensitive information on a website from a QR code. Instead, navigate directly to the official website.

# Malicious Mobile Device Apps

It is not recommended to install apps from outside of your device’s official app store. Doing so puts you at much greater risk of encountering malicious apps. However, even the app stores themselves are not perfect at preventing malicious apps. Here are some ways you can protect against malicious mobile apps that could have made it to the app store:

* Before installing any apps, do a safety check: Are the reviews positive? Are there many downloads? Do the permissions the app requires make sense?
* Make sure you have a lock screen configured that requires a passcode, thumbprint, or face recognition to unlock. This helps protect your phone, data, and accounts against unauthorized access.
* Delete apps you no longer use. This reduces your attack surface.

# Web Browsing

**Poisoned search results lead to malware/credential theft**

Sometimes top search engine results for software downloads, document templates, and other things can lead to websites with malware instead of the expected program or document. If you search for and download software, before you launch the software installer, scan it using the [VirusTotal](https://www.virustotal.com/) service which will check it with 70+ different antivirus engines. Only use VirusTotal to scan non-sensitive things, like software downloads; do not use it to scan anything that should not be public, as submitted files are made available to others.

Other poisoned search results can lead to fake websites that will capture your login credentials. Check the URL (address bar) after you arrive at a website to ensure it is the website you were expecting before entering any information. When possible, navigate directly to a frequent website instead of searching for it. Bookmark known good sites you frequent to avoid this.

**“Malvertising” AKA Malicious Advertisements**

Hijacked or paid malicious advertisements can direct you to malicious sites to install malware, steal login credentials, or other perform other unsavory action. This is a variant of the above “poisoned search results” and can be avoided in the same ways. Lately, “Sponsored” search results (the first result, a paid advertisement) for common software have led to malware. In addition to the above suggestions, you can also avoid clicking sponsored results as you know it is an advertisement and the actual website is further obscured.

**“Antivirus” Scareware**

These are websites that have a full-screen pop-up telling you that “Your PC is infected! Call us at phone number \*\*\*-\*\*\*-\*\*\*\*”. There is often even audio to alarm you further as well as images/videos depicting antivirus scanning and malware activity. If you call, they will ask you for payment, information, and ask you to connect from your computer to a remote support service where they can see and control your computer. This can lead to malware, identity theft, and fraudulent charges. I am not aware of any Antivirus that will pop-up and ask you to call a number for assistance in this manner. Should you come across this scam, you can just close the window and/or reboot your computer to make this go away.

**Browser Update/Additional Software Required**

Should you receive a notice you need to update your web browser to view the content, close your browser. This is a scam that leads to malware.

**Malicious Downloaded Documents**

A downloaded document should not contain a CAPTCHA (“Are you a robot?”). If it does, it is fake and clicking it will lead to a malicious website. Do not click. Instead, close and delete it!

# Phone Calls

**Social Engineering Phone Calls**

Social engineering involves interacting with individuals from an organization (by phone call for example) and trying to trick them into performing actions that might are harmful to the organization. Some examples goals might include changing information in IT systems (such as banking information), divulging sensitive information, changing passwords, navigating to malicious websites, running malicious code, etc.

Hackers have increasingly been using this tactic to achieve their nefarious goals. A group known as “Scattered Spider” have been using social engineering phone calls against various organizations including some in northeast Ohio. You might have recently heard about hacking of the companies Caesars Entertainment and MGM Resorts that resulted in significant downtime due to attacks from this group. Be aware that hackers do not only hide behind computers but might also call, so be on guard and watch out for calls that do not seem right.

**Caller ID Spoofing**

Caller ID does not necessarily give you correct information about who is calling. Caller ID can be spoofed to provide an incorrect phone number. You have probably seen this with junk calls appearing to come from a local phone number in order to make you more likely to answer it. Sophisticated scammers might spoof a known entity’s phone number to impersonate them. One example involves using the caller ID of a local police station, claiming that you need to pay a fine to avoid an arrest warrant.

**AI voice replication**

A few seconds of audio recording of a person speaking is sufficient to train to AI to be able to create realistic fake audio that convincingly sounds like that individual speaking. This fake audio can be used to conduct extortion, to impersonate a person in a position of authority to request a wire transfer or other sensitive action, etc. To work around these, contact the individual at a known contact number or have procedures in place for extraordinary circumstances.

**Callback Phishing - Fake orders with callback phone number**

Many phishing email that use a theme of a fake order with a shockingly high price tag. These emails contain no links and have only a phone number to “cancel your order”. When a person is directed to a phone, they might be more likely to let down their guard. Unfortunately, there are some call centers staffed with scammers who will take advantage of you. Most if not all real online orders will have links pointing back to the website and rarely have a phone number. If you are not sure if the email is real, you can always check your credit card transactions to see if a charge really occurred.

**Fake Tech Support Calls**

Scammers claiming to be from “Microsoft” or other companies will call, telling you they have detected malware on your computer. They will ask you for payment information and ask you to connect to their remote-control website. This is a scam – Microsoft will not proactively call to help clean-up malware.