# Scam Safety

## Phishing Scams

Phishing involves someone contacting you to steal sensitive information or get you to send them money.

### Common Phone Scams

- Claiming to be law enforcement and threatening to arrest you unless you pay now over phone.
- Claiming to be from IRS and asking you to pay owed taxes/fees over the phone immediately.
- Claiming you won a vacation or prize but must pay them a fee to complete the process.

### Phone Scam Facts

- Debt collectors / government workers can't threaten or force you to do something over phone.
- IRS will contact you by mail if you owe taxes, and won't ask you to pay over the phone.
- Real government agencies won't contact you for your Medicare number.
- Law enforcement won't call to demand you send them money.

### Common Email Scams

- Claiming to be family or friend asking you to purchase gift cards for them.
- Claiming to be your bank and asking for pin code or social security number.
- Claiming to be a service you use and asking to give them passwords or credit card information.

### Email Scam Clues

- Odd typos in the email address. For example, Bank of America but address is *@bankofamercan*
- Unusual grammar and typos; scammers message many people and attempt to get money fast.
- Pressure to act quickly; using phrases like ASAP, this is urgent, you must act now, and so on.

### Scam Protection Tips

If suspicious, hang up phone or don't respond to email. **Find the official number or email for the organization and contact them yourself directly to clarify the matter.** Don't use contact info given by suspicious source.

- Try not to send money over the phone or email
- Don't give financial information like bank account numbers or pin codes to unknown sources.
- Don't give personal information like Social Security or Medicare numbers to unknown sources.

# Online Safety

**Malware** includes viruses or unwanted software that is secretly installed onto your device. While it sounds scary, you can reduce the chance of being infected by studying up on best practices in the resources below.

## Virus Protection Tips

- Use well known programs and avoid downloading free software from suspicious looking sites.
- Pay attention to security warnings from your internet browser.
- Don't click on pop-up ads or links sent to you from unknown sources. Instead, search for the website yourself using a trusted search engine like Google.

## Virus Removal Tips

- Check software is up to date
- Download security software to scan and remove viruses, if not already installed.
    - Do your research as there are fake security software scams
- Worst case, you may need to re-install your computer operating system to start fresh.

# Resources

## Identity Theft Reporting

Report possible identity theft or stolen information here: ***https://www.identitytheft.gov/#/***

## Free Online Safety Courses

Federal Trade Commission consumer advice articles cover online privacy and how to avoid online scams:

***https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security***

Digital Learn provides free online teaching of basic technology topics, including online frauds and scams:

***https://www.digitallearn.org/courses/online-fraud-and-scams-new***

GCFGlobal offers free online tutorials for learning all sorts of skills, including internet safety:

***https://edu.gcfglobal.org/en/internetsafety/***

## Lake City Community Center Tech Help

In-person tech help on Wednesdays and Fridays from 9am - 3pm at the Lake City Community Center.