LIBRARY FREEDOM PROJECT

DIGITAL SCAMS AND FRAUD

Scamming is a growth industry. Advances in technology, as well as the widespread availability of personal data online, have created an explosion in online scamming and fraud. Know how to spot these scams and what to do if you become victim to them.

SOME TYPES OF SCAMS

Imposter scams

- You get a call about a fake insurance claim, warranty, health care issue, tech support, etc
- The scammer wants you to believe there's an issue you need to address immediately
- These scams intend to make you reveal personal info (also known as "phishing")
- Some use AI voice cloning to mimic the voice of a friend or loved one in trouble

Invoice, bill, debt, or advanced fee fraud

- These email scams want you to think you owe money and are in danger if you don't pay up
- Something about these messages is usually "off" - the email address is strange, the body of the message has typos or other errors, or it looks copy/pasted
- Often, any links or attachments are malware that can infect your computer - DON'T CLICK!

Fallout from data breaches

- If your personal info was compromised in a data breach, scammers may take advantage of that with fake emails from companies impacted by the breach, or use your compromised data to initiate one of these other scams

Scareware

- Urgent messages that appear as pop-up ads on a user's computer
- Intended to make the user think their computer is infected with malware or a virus

IF YOU GET SCAMMED: FTC CONSUMER PROTECTION

- **Report fraud:** ReportFraud.ftc.gov
- **Report identity theft:** www.identitytheft.gov
- **More resources:** consumer.ftc.gov/scams

PROTECT YOURSELF

Remember that **scammers use emotion as a tactic**

- Stay calm
- Hang up the phone, leave the computer
- Call someone you trust
  - Do you know someone savvy with tech?
  - Try calling your local librarian!

Use **strong, complex passwords**

- Store passwords in a password manager
- Use 2-factor authentication for more safety

Run **software updates** for the latest security

Use an **ad-blocker** to avoid malware

Make sure websites you visit use **HTTPS**

Check to see if you've been caught up in a **data breach** at: haveibeenpwned.com

Be cautious when opening emailed links or attachments, or when answering calls from unknown numbers

Use a safety phrase with family, friends, healthcare providers, etc

- If they call you, **ask for the safety phrase**

libraryfreedom.org info@libraryfreedom.org

Created with support from the Rose Foundation for Communities and the Environment