

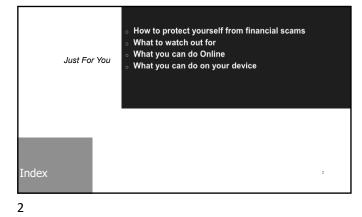
You may have heard about recent scams involving gift cards, cryptocurrency, wires, Zelle® or other third-party payment apps. We wanted to share a few things to look for, as well as some tips to protect yourself and your money.

How to protect yourself from financial scams

4

Providing Employee Benefits to the Plumbers of New York City si	nce 1946
	4

1



Impersonating a Fund Office employee –

A scammer may call, email or text you pretending to be from the Fund Office. They may say there is fraud on your account or try to trick you into providing personal information in order to gain access to your account.

What to watch out for

5

Fund Office employees will **never** ask you to transfer money to yourself as a way to resolve fraud. We'll also **never** ask you to share a one-time passcode or your username and password. Providing Employee Benefits to the Plumbers of New York City since 1946 Keep in Mind

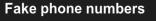
Unusual requests for sending or transferring money!

Fraudsters may try to trick you into thinking you have fraud on your account. To reverse it, they suggest you transfer money "to yourself" when, in fact, the account you transfer money to belongs to the scammer.

6

What to

watch out for



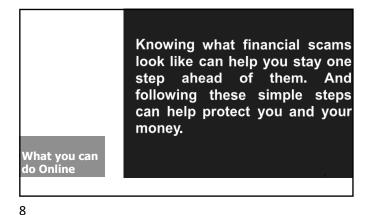
Scammers sometimes use technology that "spoofs" phone numbers. That means the Caller ID indicates that the call is coming from Fund Office, even though it's not.

What to watch out for

7

What you can do Online

10



Use Multi-Factor Authentication

Use Strong and Unique Passwords

Use letters (both upper and lower case),numbers,

Don't use letters and numbers in sequence (no "abc", "567", etc.). Use 14 or more characters.

Don't write passwords down. Consider using a secure password manager to help create and track passwords. Change passwords every 120 days, or if there's a security breach.

Don't share, reuse, or repeat passwords.

Don't use dictionary words.

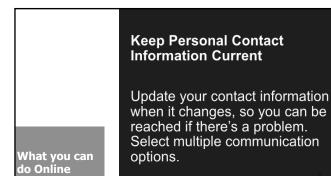
and special characters.

Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).

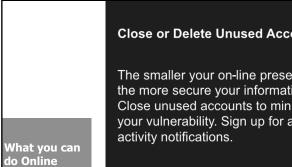
What you can do Online

11





9



13

Close or Delete Unused Accounts

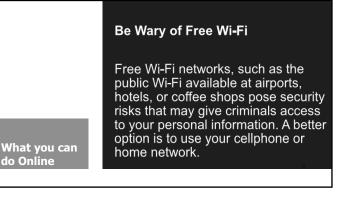
The smaller your on-line presence, the more secure your information. Close unused accounts to minimize your vulnerability. Sign up for account

Use Antivirus Software and Keep Apps and Software Current

Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

16

What you can do Online



14



The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:

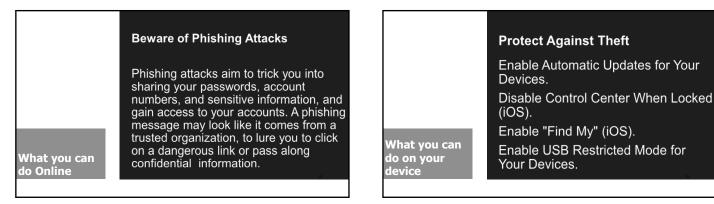
» https://www.fbi.gov/file-repository/cyberincident-reporting-united-message-final.pdf/view >> https://www.cisa.gov/reporting-cyber-incidents

17

18

What you can

do Online



	Limit Software Exploits
	Disable AirDrop (iOS).
	Disable Bluetooth When Not In Use.
	Disable JavaScript (in browser of choice).
What you can do on your	Disable Personal Hotspot When Not In Use.
device	Periodically reboot the device.

19

20

What you can do on your device

Protect Your Communications

Disable Handoff (on iOS devices). Hide notification previews when your devices is locked.

Disable calls on other devices.

Disable "significant locations" feature.

Disable text message forwarding.

22

	Review for Compromise
	Review Google Maps location sharing (do you want your location to be shared in real time). Review "Find My" location sharing (iOS) devices.
	Review alternate Face ID (iOS) settings.
	Do you want others to be able to access your phone via Face ID?
	Look for suspicious configuration files (iOS) within Settings.
What you can do on your device	Remove unknown devices from iCloud (iOS).

Prevent Ad Data Leakage Disable tracking across apps on your iOS device. Disable personalized ads. Disable loading of remote e-mail images. What you can Disable Siri (or other) data sharing on your devices.

23

do on your device

Protect Wireless Data Disable Wi-Fi Sync on your iOS device. Limit Bluetooth access for Apps. What you can do on your device

Use 2-step verification

Encrypt your messages (use Signal or WhatsApp or some other secure messaging app to communicate sensitive information).

24

What you can do on your device

Title goes here

	Secure Online Accounts
	Do a security checkup (on your Google account).
	Turn on two-factor authentication (for your Google account and your Apple and Facebook and any other online account that supports it).
What you can do on your device	Control your visibility on Facebook.
	Turn off or limit your off Facebook activity.

25

It Won't Happen to Me

Assume your device and your activity are worth surveillance by a malicious actor. Because they are. You may be the way they attack a web site or network that has more valuable data than you imagine. Don't be the weak link in the chain.

28

What you can

do on your device

Network SecurityWhen sharing photos, recognize you are
sharing metadata about that photo (location,
date and time). Strip that meta data if you do
not wish to share it. Use a DNS over HTTPS
extension as DNS queries are clear
(meaning anyone can see them). Cloudflare,
Google and Qad9 all offer DNS resolvers
that offer some encryption and share little
information about your DNS queries. Enable
or use a secure browse. Use a Personal
VPN service.

26

Do not use pirated or "cracked" software

Use of pirated or cracked software (software obtained outside of the App Store in the Apple universe or even within the Play store in the Android universe) can lead to the delivery of malware onto your device. That could lead to the siphoning of sensitive or private information from your device. It also could lead to information being shared that allows malicious actors to then hijack your financial, health, benefit or other private accounts online.

What you can do on your device

29



27

Do not use pirated or "cracked" software

Use of pirated or cracked software (software obtained outside of the App Store in the Apple universe or even within the Play store in the Android universe) can lead to the delivery of malware onto your device. That could lead to the siphoning of sensitive or private information from your device. It also could lead to information being shared that allows malicious actors to then hijack your financial, health, benefit or other private accounts online.



info@nypl1f.org

If you think an email, call or text is suspicious, call us directly at the Fund Office (718) 223 – 4313 so we can help.

31

