# Internet Scams & Phishing

Ashby Village & U.C. Berkeley Retirement Center
Sam Duncan, Maryl Gearhart & Hilary Naylor
with Pat Hom & Celie Placzek

**February 20, 2020**

## TYPES OF SCAMS & PHISHING

| Email examples | Common email features |
|---|---|
| **The urgent request**<br>*"Restart your membership now."*<br>*"Update your personal information now."*<br>*"Confirm your account immediately."*<br>*"Your account has been suspended."*<br>**Come-ons that ask you to click...**<br>*"Just take this short survey. Click here."*<br>**Unexpected refunds, payments, or rewards**<br>*"Tax refund!"*<br>*"Refund due to system error"*<br>*"Redeem your reward!"*<br>**Requests for money**<br>for emergencies or urgent needs<br>from strangers, 'relatives,' 'friends,' unfamiliar charities, or police<br>often from overseas | ● from a company or agency you trust (e.g., "Netflix," your bank, or the "Social Security Administration")<br>● bogus email sender (*not* from the company)<br>● generic greeting (e.g., "Dear customer")<br>● reference to "your card" or "your account"<br>● request to click<br>● conveys urgency<br>● errors in spelling or grammar<br>● unprofessional formatting |

| Browser pop-up examples | Common pop-up features |
|---|---|
| **Your computer needs repair**<br>**Ransom demanded** | ● from a company or agency you trust ("Microsoft" or "Apple" or "Department of Justice")<br>● request to click or call<br>● conveys urgency<br>● request for money<br>● errors in spelling or grammar<br>● unprofessional formatting |

## WHAT TO DO WHEN YOU'RE CONCERNED

### If you think an email or pop-up is suspicious:

*Think before you act. There is no rush.*

*If in doubt about email, throw it out!* Mark it as Junk or Spam.

*If in doubt about a pop-up:* Delete browser history.
Close browser & restart computer.
Block pop-ups.

*If unsure, contact a company or organization:*

Look at company website - are they actually offering or requesting something?
You could call the organization to inquire.
You might forward to abuse department.

### If you clicked a suspicious link

*Don't panic, and don't be embarrassed.*

*Document* what you see on screen: Take a photo or write down.

*Change email password.*

*Delete browser history, shut down browser, and restart.*

*Request help.*

*If financial accounts are at risk:*
Watch for unauthorized charges.
Change account passwords.
Contact your financial institution to close the account.
Let your financial institution know.
Consider filing a report to police.

### If you're infected with ransomware:

Document what you see on screen: Take a photo or write down.
Do not touch any buttons.
Request help immediately from a tech professional.

## WAYS TO MINIMIZE RISKS

Update regularly your OS (operating system), browsers, and apps.

Back up regularly.

Use complex passwords, and different passwords for each account.

Mark suspicious emails as junk/spam.

Block pop-ups on browsers.