SCAMS!

Melissa Dubinsky & Paulette Woolf

1. Phishing
2. Common scams
3. How to avoid scams and protect yourself
4. Finished with your phone?
5. Helpful tips
6. Keep a record of everything
7. Stay on top of your financial security
8. Key messages

What is a Phishing attack?

- Phishing is when a fraudster contacts you pretending to represent a trustworthy source, like your bank or other legal entity, and uses what they already know about you to build trust and get more information from you.
- They may pressure you to act quickly. And spotting the real versus the fake can be hard.
- If a request seems suspicious or you don't understand why you are getting it, call the company directly at the number listed on its official website or on the back of your credit or debit card.

  Don't use the number "helpfully provided" by the fraudster.


Your PayPal Access Blocked !

PayPal

Your PayPal Account is Limited, Solve in 24 Hours!

Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer.
Click here to fix your account now.

Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now

Impersonation scams

- Scammers pose as a legitimate company and request personal information or a payment transfer in order to make things "right" on your account
- May use a fake caller ID that could show up as a legit company's number
- May request remote access to your device
- Scammer posing as a utility company might warn you to pay your balance (to them by giving a credit card or bank details) within a limited time or else the utility will be shut off

The 2020 Twitter Bitcoin Scam (Celebrity Account Takeover

- **Attack**: Hackers used **spear-phishing** to trick Twitter employees into giving up login credentials.
- **How It Worked**:
  - Posed as IT staff in a phone call + fake login page.
  - Gained access to **130 high-profile accounts** (Elon Musk, Barack Obama, Apple).
  - Tweeted: *"Send Bitcoin to this address for double your money!"*
- **Impact**:
  - **$118,000 stolen** in Bitcoin (FBI).
  - **Teen hacker sentenced to 3 years in prison** (BBC).

Actual Example of a Phishing Attack

Fake "Netflix Account Suspended" Email (2024)

- Claims your subscription is "on hold due to payment issues”
- Urges you to click a link to update billing info
- Support@netflx.com-support
- Netflix.billing-update.com
- Stole credit card details and Netflix credentials.

Consequences of sharing personal identifying information

According to a 2023 FBI Report:

Phishing was the

#1 cybercrime,

with $10.3B in losses

More Examples

Phone scams

- Often involve high-pressure pitches, with **threats of fees or even jail time** if you don't comply with a scammer's demands
- Scammers may try to pressure you to:
  - Sign up to buy products or services, like extended warranties
  - Hand over personal information such as for a fake lottery winning

Grandparent scam

- You receive a call or text message from someone claiming to be a grandchild or loved one or on behalf of that person
- They have a lot of detail about that person and their relationship to you
- They ask for money to help with an emergency, plus instructions on where to send the funds
- Never send funds without checking with another person – the loved one’s parent, spouse, etc.

CBC Investigates: Grandparent scams steal millions from seniors. Organized crime made Montreal a hotbed for them

The group, and 17 other Canadians — nearly all from the Montreal area, and many from the West Island suburbs — was part of an elaborate international scam network that defrauded hundreds of American seniors out of a total of more than $21 million US.

They were placing phone calls to "elderly victims in Virginia," pretending to be their grandkids and asking for money.

Fake friends scam

“How are things in Israel?”
“ Great. Sara just got married”

- If you receive a direct message or a “follow” or friend request from someone you don’t know, be careful. If you respond, hackers gain access to directly send malicious links. If you don’t recognize the person, or the link looks suspicious, don’t respond. Delete the message or request.
- Strangers aren’t all you have to worry about. Hackers will check to see whom you are friends with, then impersonate them. So if your Aunt Molly reaches out to you asking for money or trying to get you to click on a link, check with her first to confirm whether it’s real or fraudulent.

The "Facebook Long-Lost Friend" Scam (UK, 2023)

- **How It Worked**:
  - Scammers cloned profiles of real people, then messaged their friends:
    - "I'm in trouble abroad—can you wire me £2,000?"
    - "My account was hacked—I need help recovering it."
- **Outcome**:
  - **£27M lost** in the UK in 2023 (Action Fraud).
  - **BBC Investigation** exposed a Nigerian crime ring behind the scams (BBC, 2023).
- **Verification Tip**: Call the friend on a known number before sending money.

Tech support scam

- Don't allow remote access to anyone who calls you asking to fix computer defects or malware
- Only deal with someone you have called directly
- Scammers like to say they are calling from a company with a program you have – like Microsoft – and tell you that you have a problem with that program and they can fix it for you on-line

Charity scams

You receive a request to donate to a charity that you've never heard of (or sounds familiar) and for which you can't find an official website

They "helpfully" send you a link to make the payment directly

Never click on a link sent to you, even from a "legitimate" charity.

Go on the website to make payments

Now that we know about the different type of scams……

What do we do about it?

SLOW DOWN

VERIFY

STOP

Financial scams – banking or tax authority

- Trying to get personal information including bank account number and password
- Emails or calls pretending to be from your financial institution (bank, IRS, BL) asking you to confirm the details of your account number
- Watch for emails that come from addresses that don't match the names of the companies supposedly sending you the emails. Keep in mind, phishing emails may use official logos and headers. One letter may be changed in the official email, most people don't notice.
- Always sign in to your financial institution's page directly.

How to avoid scams and protect yourself

Be vigilant on social media and across the web

Never use gift cards to make payments (they are only for gifts)

Don't fall for fake merchandise scams. Beware of low-quality or altered images or faked endorsements. In general, if a deal sounds too good to be true, it probably is.

Never share personal, banking or password information on social media.

Even a fun quiz that creates your superhero name using your mother's maiden name can be used to target your accounts.

Phony apps scams

- Hackers can attempt to access the data on your phone through potentially harmful apps.
- If you download one to your mobile device, your personal information could be exposed.
- These fake apps are sometimes installed by clicking on a link or pop-up ad, but they may also be available in your phone's app store, like Google Play.
- If you're not sure an app is safe, do a quick internet search about it and the developer before you download and install anything.
- Some companies take over the connection you are trying to make – you enter a hotel chain name and something like Booking.com takes over. You might sign with the alternate app without realizing it.

How to Avoid Fake Friend Scams

- ✅ **Reverse-image search** profile pics (many use stolen photos).
  ✅ **Never send money** to someone you've only met online.
  ✅ **Verify emergencies** by contacting family/friends directly.
  ✅ **Report suspicious accounts** to the platform (Facebook, Tinder, etc.).

Clear your phone when you are finished with it

- When it's time to get rid of your phone, make sure you erase all your personal information. If you don't, you could leave yourself vulnerable to identity theft. Everything from your address to your bank info could be on your phone.
- To erase your phone, look on the manufacturer's website or check with your service provider for instructions.

Helpful Tips

Keep a record of everything if you are subject to identify theft

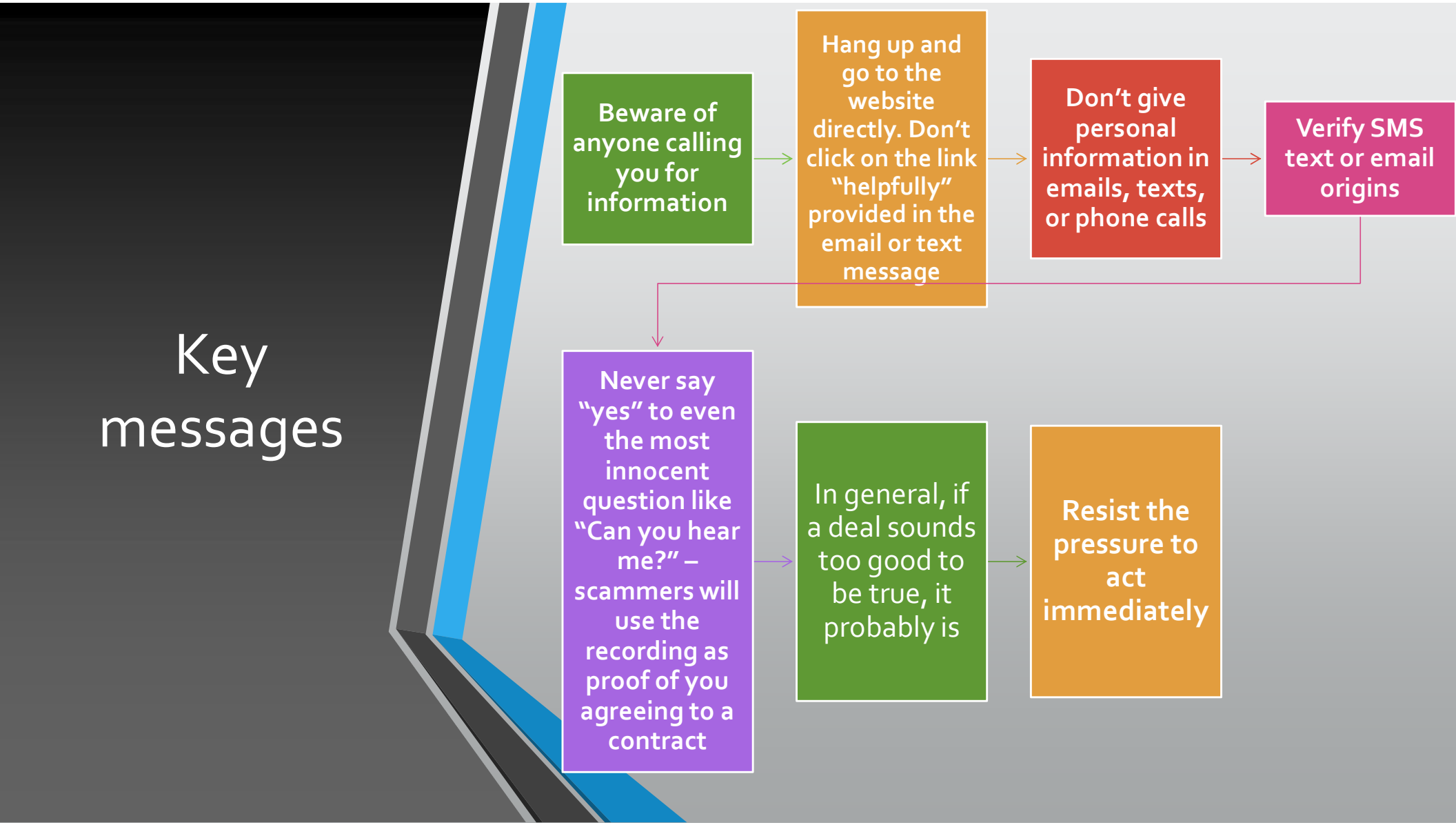
Staying organized can help make your identity theft recovery as smooth as possible. Keep a record of information related to the theft, including:

- ✓ Digital or hard copies of emails
- ✓ Notes from phone conversations with creditors
- ✓ A list of banks or agencies you contacted, including dates, times, who you spoke to and contact numbers
- ✓ Any mail or additional documentation

Stay on top of your financial security

- Monitor your credit through credit reporting agencies
- Dispute any inaccuracies, even small ones. Small ones can be a test before a large withdrawal is made

Key messages



Update Security software on phone and computer frequently in response to hacker activity

Password Protect your phone

Use a secure password or a password manager

Identify for yourself, ahead of needing one, an IT professional to help you if you click when you shouldn't or otherwise need help.

Thanks for listening

Information taken from CapitalOne – more information can be found at **www.Capitalone.com/stopscams**