Dedham Savings

WELCOME!

Financial Wellness Seminar

Protect Yourself from Fraud

Housekeeping

- Restrooms
- Refreshments
- Questions

Dedham Savings

Today's Presenters:

- **Carol Lewis, Esq.**
  Senior Vice President
  Compliance Officer

- **Mike Murteira, CISSP**
  Assistant Vice President
  Information Security Officer

- **Laura Hickson, CAMS**
  Vice President
  BSA & Security Officer

Dedham Savings

What is Fraud?

- Illegal, unauthorized, or improper act or process of an individual that uses the resources of an individual for personal benefit, profit or gain

- Actions that result in depriving a person of rightful access to or use of benefits, resources, belongings, or assets

Who is at risk?

- Anyone can be a victim of fraud
- Most vulnerable groups:
  - *Seniors*
  - *Military Personnel*
  - *College Students*

Who are the fraudsters?

They could be people you know, such as:

- Family members & caregivers
- Friends, neighbors, or acquaintances
- Agents under Power of Attorney
- Financial Advisors

Who are the fraudsters?

They could be strangers posing as:

- Telemarketers
- Utility companies
- Computer experts
- Home repair contractors
- Medicare scam operators
- Friend or family in need of help
- Government/IRS officials
- Financial institutions

Fraudster Tactics

Claim they need money for an emergency surgery or medical bill

Request money for fees, debt assistance, or threaten to shut off services unless payment is received

Request money for travel expenses or documentation so that they can visit you

Dedham Savings

Fraudster Tactics

Seek smaller loan amounts and later ask for larger amounts

Ask for gift cards & wire transfers (because they are hard to trace & not retractable)

Dedham Savings

Latest Scams

- Impersonation
- Grandparent
- Romance/Friendship
- Disaster Relief/Charity
- Computer

Impersonation Scams

The Fraudster relies on your relationship with your Bank:

- Pretends to be from department (*e.g.*, fraud) at Dedham Savings
- Has some personal information about you
- Gains your trust
- Tells you there is serious problem that must be addressed immediately
- Convinces you to give them credentials so they can access into your account

Grandparent Scam

Fraudsters:

- May know grandchild's name
- Usually cry to disguise voice
- Plead for victim to send money via wire transfer, gift cards, check, etc.
- May ask that you not tell family members or your bank
- May have a 2nd individual pose as an official who can validate the claim

Romance/Friendship Scam

The fraudster is seemingly seeking companionship, but they just want your money. How the scam works:

- Fraudster creates a fake profile to court victims online
- The relationship moves fast & trust is gained
- The fraudster asks the victim for money, receives it, and vanishes

Disaster Relief Scam

- Fraudsters may pretend to be safety inspectors, government officials trying to help you, or utility workers who say immediate work is required.
- Unlicensed contractors and fraudsters may appear in recovery zones with promises of quick repairs or clean-up services.
- Fraudsters know people need a place to live while they rebuild. They'll advertise rentals that don't exist to get your money and run.
- Fraudsters will often try to profit from the misfortune of others, sometimes using familiar-sounding names or logos.

Disaster Relief/Charity Scam

Fraudsters want your money quickly. Charity scams often pressure you to donate right away. Tips:

- Tell caller to send info via mail
- For requests received by mail, do your research
- Rule out anyone who requests cash, wired money, or pre-paid debit/gift cards
- Use extra caution during disasters or holidays

Remote Access Computer Scams

1

Be cautious of scammers posing as tech support online. Use the tech support listed on a software package or on your receipt

2

Do not rely on caller ID alone to authenticate a caller

3

Do not give control of your computer to a third party

Cyber Fraud

Fraudsters use various tactics, techniques, and procedures to steal Non-Public Personal Information (NPPI).

- NPPI can include Social Security numbers, account/credit card numbers, and more.
- Value of NPPI on the Dark Web (from privacyaffairs.com)
  - *Social Security Number $2*
  - *Credit/Debit Card Information $14 - $240*
  - *Online Banking Credentials $40 - $120*
- Information can be used to gain access to accounts, extort victims/companies, and steal identities.

Dedham Savings

Phishing

Fraudsters will use emails, phone calls, and text messages to trick you into giving them your personal information.

How to Recognize a Phish	How to Protect Yourself from a Phish	What to do if you Respond to a Phish
Are you being asked to either click a link or open an attachment?	Install security software & latest OS/app patches Look into Multi-factor Authentication (2FA/MFA)	If NPPI is shared, report it on IdentityTheft.gov If a link or attachment was opened, scan for problems

Phishing Example

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

1 Suspicious email address.

2 Threatening language.

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

3 Threatening language.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify..

Verify Now

4 Suspicious link.

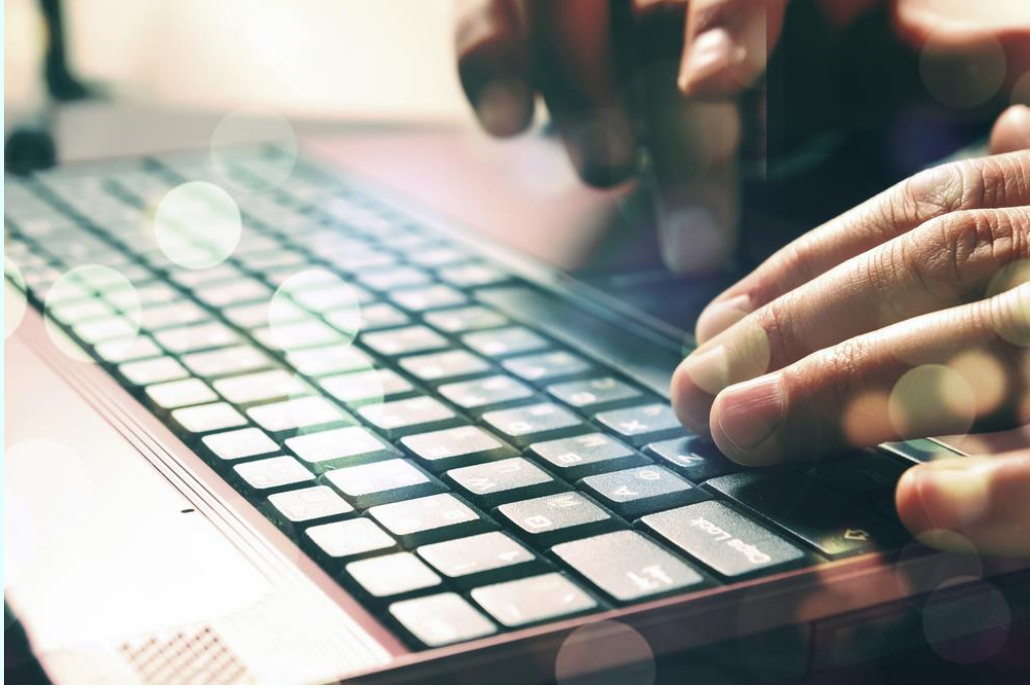
5 Odd capitalization and punctuation.

Microsoft Security Assistant
Microsoft office365 Team!

Dedham Savings

Malware

Malware (e.g., viruses, spyware, ransomware) is one of the biggest threats to device security.



How Malware Gets on Your Device	How to Know if You Have Malware	How to Prevent Malware	What to do if Malware is Found
Open or download attachments or files from emails or websites	Look for unusual behavior on your device	Install security software and latest OS/app patches	Clean device (do it yourself or bring to a professional)

Malware Example - WannaCry

Dedham Savings

Identity Theft

Fraudsters steal your personal financial information and use your identity to commit fraud and other crimes.

- Social Security Number
- Birth Date
- Credit Card/Account Numbers
- PINs & Passwords

Dedham Savings

Account Takeover

A form of identity theft where a fraudster successfully gains access to your account credentials. With this access, fraudsters can:

- Transfer funds out of your account into their own accounts.
- Order credit/debit cards and send them to their address.
- Sell credentials on the Dark Web.

In 2020, account takeover represented 54% of all fraud-related events

Dedham Savings

Identity Theft Safeguards

- Protect your personal information: Don’t leave personal documents out in plain view
- Protect incoming and outgoing mail
- Sign up for direct deposit
- Shred “financial trash”
- Monitor bank/credit card accounts

Identity Theft Safeguards

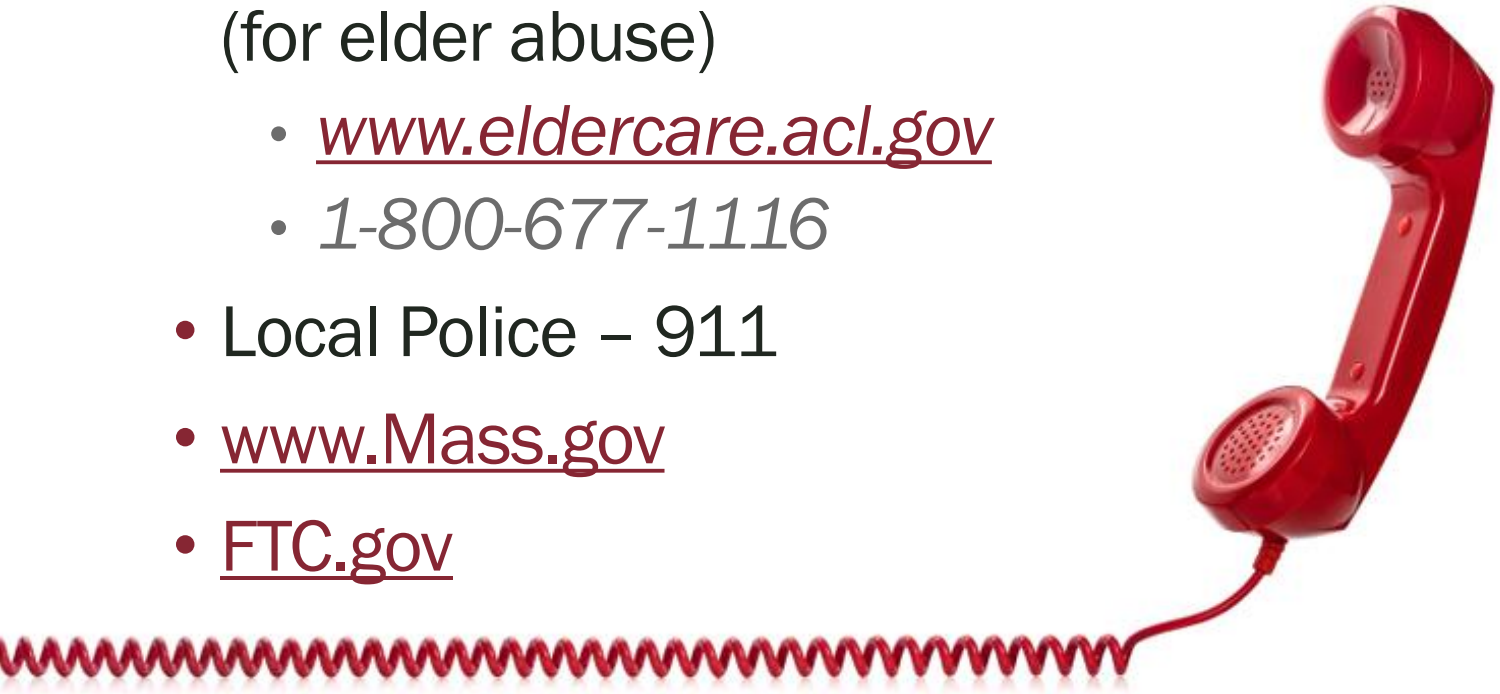
- Review credit report annually & report fraudulent activity (our mobile app provides free credit report & score anytime)
- Create strong, unique passwords for all accounts
- Enable Multi-Factor Authentication (MFA)
- Keep your devices up-to-date
- Think before you click!

Identity Theft: If You Are a Victim

Place	Request	File
Place an initial fraud alert/ security freeze with one of the major credit reporting agencies • Equifax • Experian • TransUnion	Request credit report from each agency annually (or view your report in the Dedham Savings mobile app anytime)	File a police report

Who can help?

- Trusted Family or Friends
- Trusted Bank Representatives
- Adult Protective Services (for elder abuse)
  - *www.eldercare.acl.gov*
  - *1-800-677-1116*
- Local Police – 911
- www.Mass.gov
- FTC.gov



Dedham Savings

Security Info

You can find fraud and related security info anytime at:

www.DedhamSavings.com/Security

Finishing Up

- Questions
- Flyers
- Survey

Dedham Savings

Dedham Savings

Thank you