Dedham Savings

Business Fraud

- Thank you for joining us!
- Housekeeping topics
  - *How questions will be handled (in person vs virtual)*
  - *Refreshments*
  - *Restrooms*
  - *Follow up email after presentation that will include links to information provided*

Dedham Savings

Topics We'll Cover Today

- Security Management Partners (SMP)
  - *Importance of an Incidence Response Plan*
  - *Cyberattacks*
  - *Social Engineering methods*
  - *Phishing & Ransomware*
  - *Individual responsibility*
  - *Effective passwords*
  - *Security tips when working from home*
- Dedham Savings
  - *Business Fraud Mitigation Tools*
  - *Steps to take if you suspect fraud*
  - *Cash Management Services*

Dedham Savings

Security Management Partners (SMP)

SMP

Frank Susi
Director of Information
Security & Policy

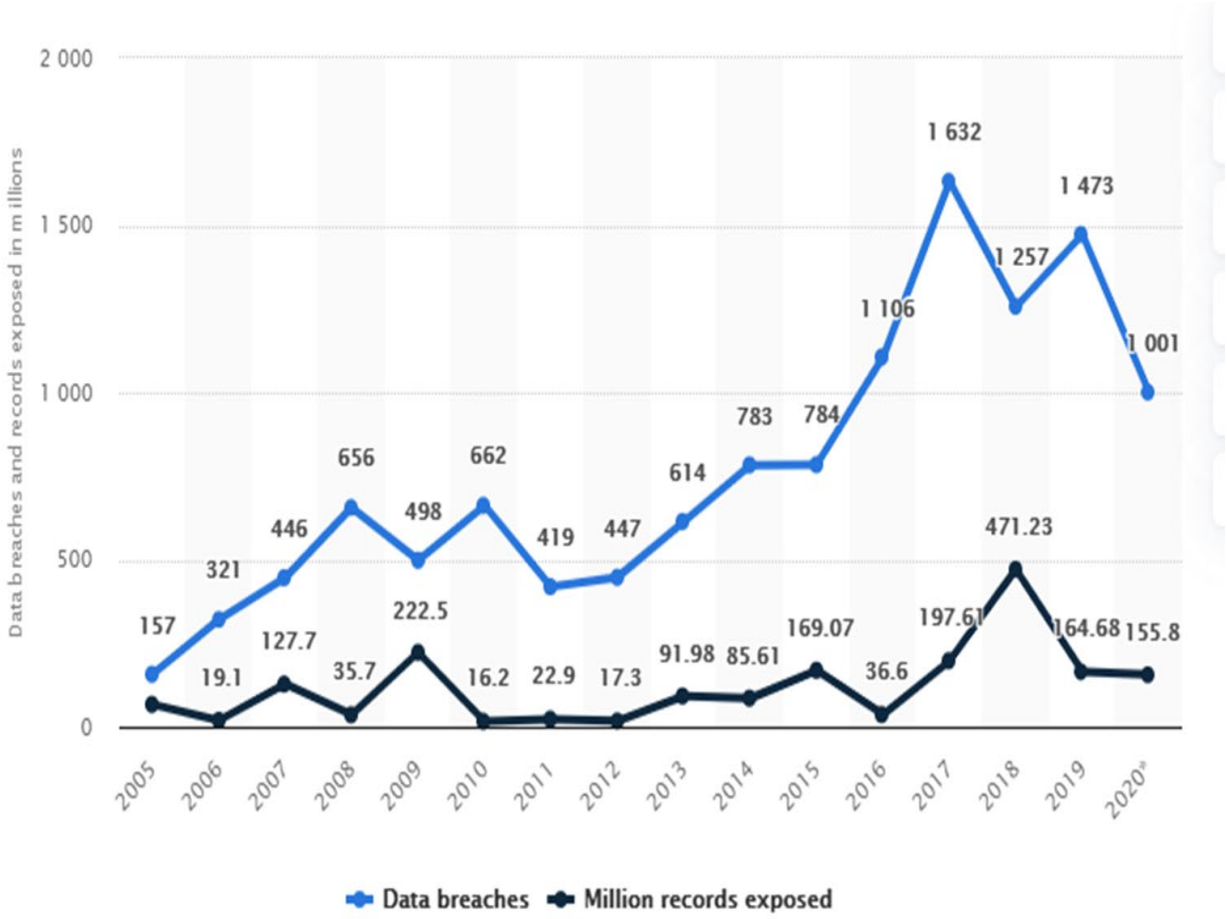
Dedham Savings

Importance of an Incidence Response (IR) Plan

- Average cost of a data breach is $4.35 million (2022)
- Healthcare industry has highest payout of $10 million average
- Average Ransomware payment increased by 71% ($925,162) from 2021 to 2022
- $17,700 is lost every minute as a result of a phishing attack
- Experts expect cybercrime damages to reach $10.5 trillion per year by 2025

Dedham Savings

Increase in Cyber Attacks



Dedham Savings

Recent Cyber Attacks

YEAR	COMPANY	ATTACK
2022	Edfinancial & OSLA	Breach of 2.5 million records containing NPPI
2022	Cisco	Yanluowang threat group successfully accesses internal network
2022	Kaiser Permanente	Exposure of 70,000 medial records
2022	GitHub	Attackers were able to download data from private repositories
2021	Kaseya	Compromise of 1,500 companies and a $70 million ransom note
2021	Pulse Secure	VPN exploit resulting in breach of defense firms and governments

Dedham Savings

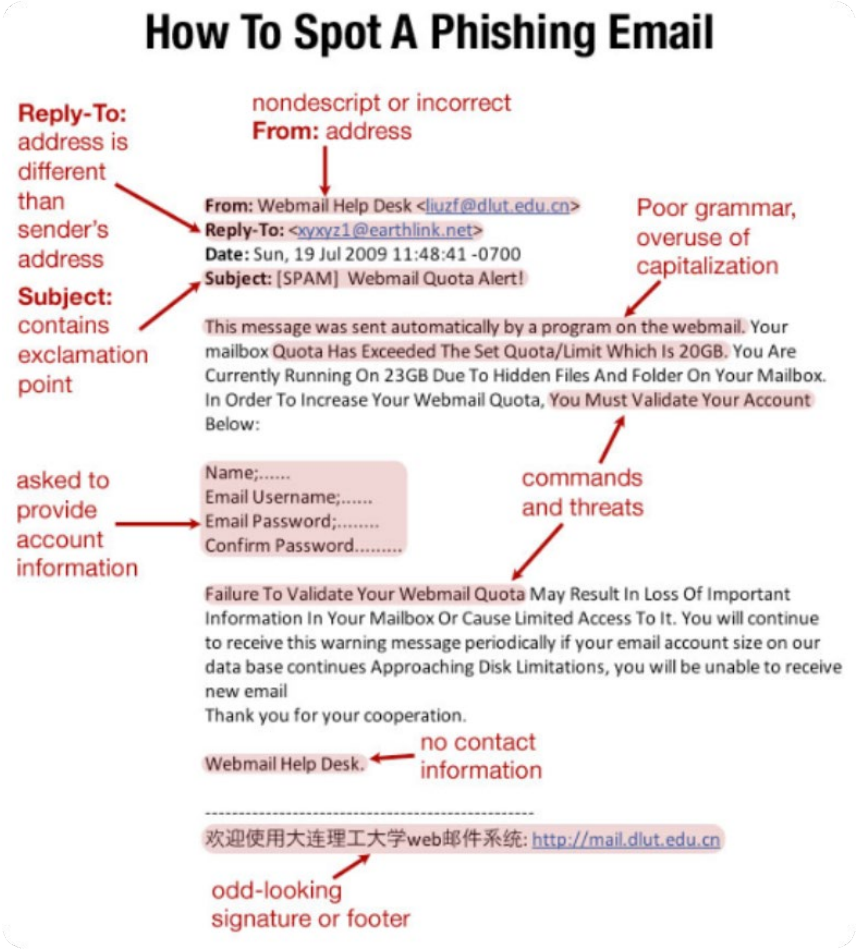
Social Engineering Methods

METHOD	DESCRIPTION
PHISHING	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information
SPEAR-PHISHING	Communication scam targeted towards a specific individual within the organization
VISHING	Voice phishing is the use of telephony to conduct phishing attacks
SMS	The act of committing text message fraud to try to lure victims into revealing account information and/or installing malware

Dedham Savings

Phishing Attacks

- Phishing is still the largest and most common method of attack
- Can appear to come from someone you know
- Can appear to come from senior management
- Can include images with malicious content to download



Dedham Savings

Ransomware

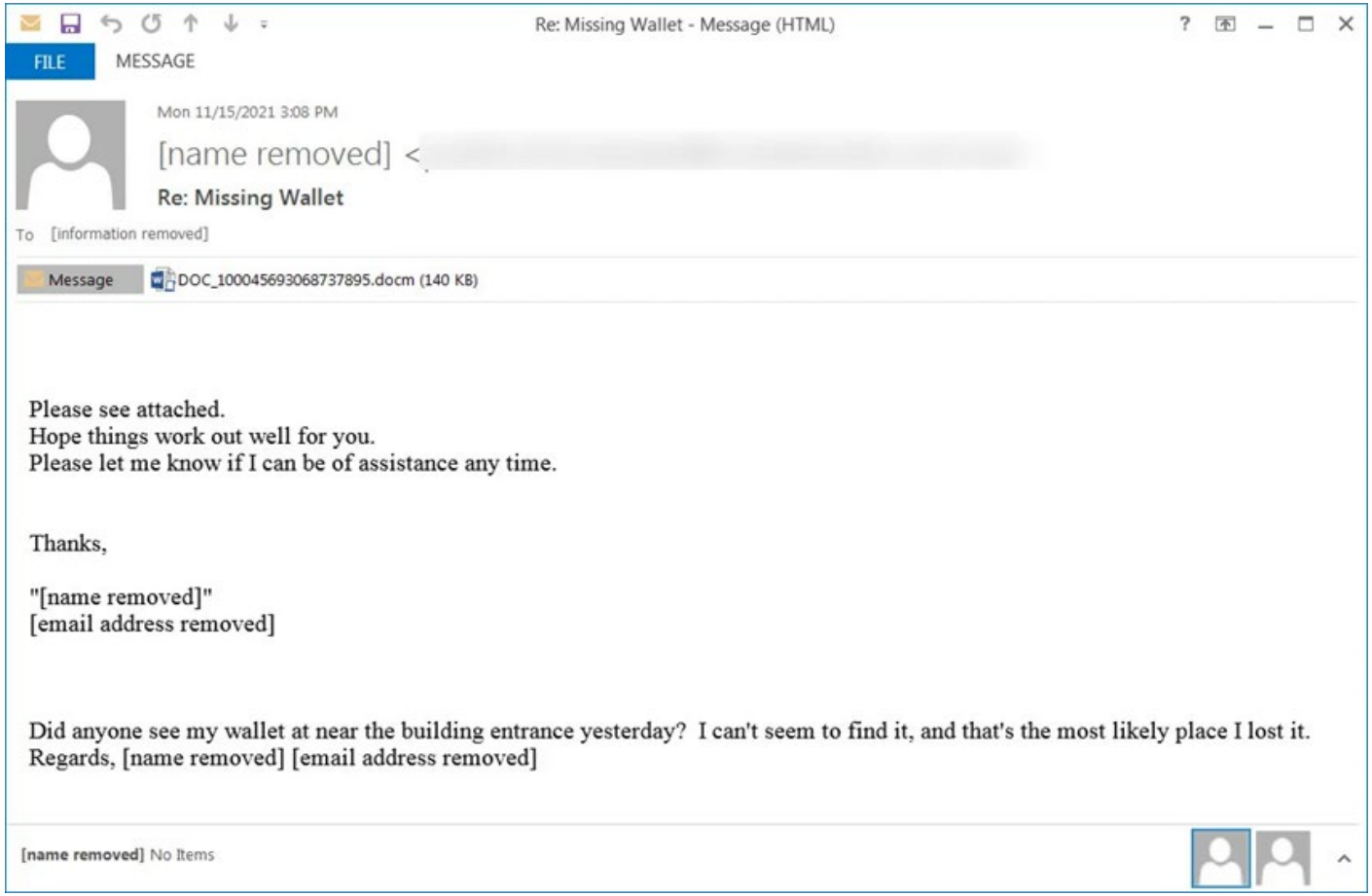
Dedham Savings

Ransomware

- Phishing emails may contain attachments with malicious code
- Once the document is downloaded and opened, the code will execute
- The ransomware will then traverse the network and encrypt as many computers as possible

Dedham Savings

Ransomware



Dedham Savings

Conti Ransomware Notice

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by
our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you
are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random
files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.onion

HTTPS VERSION :
https://contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and
are ready to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us as soon as possible.

---BEGIN ID---
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
---END ID---
```

Individual Responsibility

- One of the most important things to understand is that YOU are the target. 95% of cybersecurity breaches are caused by human error
- Passwords
  - *Make your passwords strong*
  - *Don't re-use passwords*
  - *Don't share your passwords with anyone*
- Be aware of phishing emails
- Alert IT of anything unusual

Dedham Savings

Password Strength

- Do not…
  - *Use personal information*
  - *Use your company's name*
  - *Write them down or store them unencrypted*
  - *Follow the standard format Uppercase>lowercase>numbers/special characters*
- Do instead…
  - *Use 2-factor authentication*
  - *Use a password vault*
  - *Use common phrases (easier to remember and more secure)*
  - *Use numbers & symbols mixed in to increase complexity*

Dedham Savings

2021 Top 10 Most Common Passwords

- 123456
- 123456789
- qwerty
- password
- 12345
- 12345678
- 111111
- 1234567
- 123123
- qwerty123

Dedham Savings

Tips for Browsing Safely

1	2	3	4	5
Use an Ad Blocker (Adblock Plus)	Use Chrome & Edge	Maintain skepticism	Be alert of bad referrals	Even trustworthy sites can have compromised components (banners, ads, etc)

Dedham Savings

Working from Home

- Keep work devices and personal devices separate
- Never store corporate information on personal devices
- Avoid using work devices for social networking and personal email
- Do not allow family members to use work devices
- Configure OS permissions within each device to ask for access to camera and microphone
- Use a camera cover whenever possible
- Be sure Remote Access is configured correctly

Dedham Savings

Questions?

- Frank Susi fsusi@smpone.com
- Joshua Henderson jhenderson@smpone.com

Dedham Savings

Business Fraud Mitigation Tools

- Check Positive Pay
  - *Positive Pay is an automated check fraud prevention tool*
  - *A file containing check info is uploaded into Business Online Banking*
  - *When check clears the account, check number, amount, issue date & payee are compared to uploaded files*
  - *For discrepancies, exception is created & presented to customer through Online Banking to review*
  - *Customer decides to Pay or Return item. (Includes over-the-counter checks, which are verified at the teller line)*

Dedham Savings

Business Fraud Mitigation Tools

- ACH Positive Pay or ACH Debit Block
  - *Positive Pay is an automated ACH fraud prevention tool*
  - *Allows businesses to set up companies authorized to debit the business account and/or block other companies*
  - *Businesses are sent an email alert any time an unauthorized transaction is presented on the account. Business can review the transaction & decide to Allow or Return the item*
  - *Business Online Banking offers easy online ability to make decisions about exception items & set up Rules*

Dedham Savings

Steps to take if you suspect fraud

- Business Incident Response Plan Checklist for Account Takeover
- Notify Financial Institution
  - *Review account activity*
  - *Request hold on the account*
  - *Disable online account access*
  - *Close affected accounts and open new accounts*

Dedham Savings

Steps to take if you suspect fraud

- Gather details on the fraudulent transactions and attempt to recall transactions with Financial Institutions
  - *Dates, types of transactions*
  - *Dollar amounts, other account numbers involved, other financial institutions involved*
  - *How did you discover the issue? Who reported it?*
  - *Was it online fraud? If so, what User ID was impacted? Was the User ID info shared?*
  - *Did you notice anything unusual about the login process?*

Dedham Savings

Steps to take if you suspect fraud

- Notify parties at your company
  - *Management, IT, Accounting, Corporate Security, Public Relations, Legal Counsel*
- Attempt to recover lost funds and plan for recourse
  - *Ask for assistance from you Financial Institution*
  - *Determine how to move forward with legitimate banking account functions*
  - *Contact law enforcement and file a complaint with the Internet Crime Complaint Center: www.ic3.gov*

Dedham Savings

Steps to take if you suspect fraud

- Identify vulnerability and begin to plan to remedy
  - *Update User IDs and Passwords for online access*
  - *Check computers and network for malware and viruses*
  - *Confirm with Financial Institutions that any vulnerabilities have been remedied*

Dedham Savings

Cash Management Services

- Business Online Banking
  - *Wire Transfer services*
  - *Fraud prevention*
    - ACH Positive Pay
    - Check Positive Pay
  - *Online statements*
  - *Real-Time account reporting*
  - *Internal & external transfers*
  - *ACH Origination*
  - *Bill Payment*
  - *QuickBooks*

Dedham Savings

Cash Management Services

- Business Mobile Banking & Mobile Deposit
- Remote Deposit Capture
- ZSuite: ZRent & ZDeposit
- Lockbox
- Sweep Account / Zero Dollar Account

Dedham Savings

Cash Management Team

Steven LaPierre
Assistant Vice President | Cash Management
781.320.1136
Steven.lapierre@dedhamsavings.com

Elizabeth Wrenn
Cash Management Specialist
781.329.6700
Elizabeth.wrenn@dedhamsavings.com

Dedham Savings

Dedham Savings

Thank you