

Cybersecurity and You – Be the first line of defense

FEATURING: NANCY VINER, EXECUTIVE IN RESIDENCE, AVIV GROWTH PARTNERS
TED PENFIELD, ASSOCIATE VICE PRESIDENT, INFORMATION TECHNOLOGY, CJP

MODERATOR: JEREMY YAMIN, ASSOCIATE VICE PRESIDENT, DIRECTOR OF SECURITY AND
OPERATIONS, CJP

There is a
hacker attack
every
**39
seconds**

↑ \$3.9M
Average cost of a
data breach

94%
of cyberattacks
begin with a
phishing email

Outdated and unpatched
software constitutes **22%**
of security issues

95% of cybersecurity
breaches are due to
human error

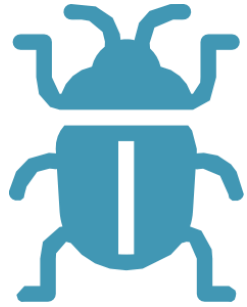
70% of
employees
don't
understand
cybersecurity

46% of websites
have high cyber
security
vulnerabilities

43% of cyber
attacks
target small
business

65% of users use
the same password
across multiple
accounts

Cyber Threats – Common Scenarios



- ▶ **Malware:** Ransomware, information stealers, banking trojans distributed via e-mail, with links or attachments containing the malicious code



- ▶ **Credential Theft:** Phishing lures individuals into exposing IDs and passwords that are reused for fraud, breach systems



- ▶ **Breach:** System is hacked and data stolen or system harmed

Social Engineering

- ▶ **Social engineering** is the art of manipulating people into giving up confidential information. Can be done via email, phone, or in-person
- ▶ **Criminals** use human nature, trust and curiosity to make a victim click on a link, download a file, reveal sensitive information, or pay them
 - Call from grandchild in trouble, need money wired
 - Call or e-mail about a debt, collections, or legal action threats



The Phish


- ▶ **Phishing** is the use of e-mail to dupe a user into revealing personal information, downloading malware, or executing a transaction
 - Looks legitimate
 - Has urgency
 - Includes links
 - Often targeted to execs




Think Before You Click!

Phishing: Stealing Your Credentials

From: Microsoft Email System <janes@cjp.org>
 Sent: Monday, August 20, 2018 10:16 AM
 To: Jane Smith <janes@cjp.org>
 Subject: A medium-severity alert has been triggered on your email account

 Office 365

A medium-severity alert has been triggered on your email account.


 **Creation of forwarding/redirect rule**

Severity: ● Medium
Time: 08/20/2018 02:16:16 pm
Activity: MailRedirect
User: janes@cjp.org

Details: MailRedirect. This alert is triggered whenever someone gets access to read your user's email.

[Investigate](#)

Thank you,
 The Office 365 Team

 Microsoft

One Microsoft Way
 Redmond, WA
 98052-6399 USA

[Privacy | Legal](#)

url=https://bonne-maman.gr/font/
 wdyvcejymexjmjtxpcjm+wgpueomnzaxttvcojgd=vba
 aciovyxxrahpsadan+=mhccmsxzpotirwpjmjgl/


someone@example.com

Password

Keep me signed in

[Sign in](#)

[Can't access your account?](#)

© 2017 Microsoft 

... But the website is
 actually fake and
 controlled by a hacker

When in doubt –
 report the email
 or call your IT
 Department

Phishing: Stealing Your Money

Hover before you click or act –
when in doubt
hover over to
review the email
address to confirm
the sender

From: Rabbi Jane Doe <ceo.verizontalk@aol.com>
Sent: Friday, March 22, 2019 3:34 PM
To: Larry Smith
Subject: Re:

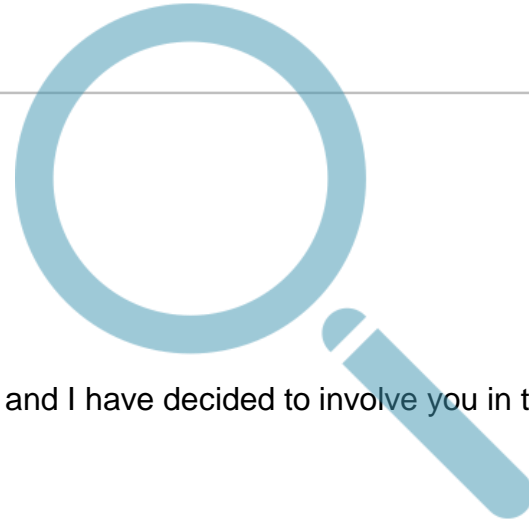
Larry,

It's the time of the year that I make donations to charity, and I have decided to involve you in this project. Because of this, I need any of the following gift cards.

- i) Best Buy Gift Card
- ii) Google Play Store Gift card

NOTE: Get physical cards, four (4) of \$500 face value each. Can you get this done in 45 minutes?

Thanks,
Rabbi Jane



Phishing Tips: Be Wary


- ▶ From an **unknown and unexpected source** asking you to perform an “urgent” action or to open a document attached to the email
- ▶ Uses a salutation such as “Sir/Madam” or awkward phrasing
- ▶ Asks you for your username and password, account number, Social Security Number (or other government identifiers) or any other personal information
- ▶ **Even if from a “Trusted Source”** don’t download or send confidential information/payments without calling the person first



Think Before You Click!

InteProIQ: Awareness Training

Become your organization's strongest line of defense

- ▶ One of the easiest and most effective things you can do
- ▶ If you can be 'phished', you can be hacked – **Awareness is the key to success** 
- ▶ Web-based training and testing platform for cyber awareness training – **7 sessions**
 - The training programs are accessible from all computers and mobile devices that use any of the popular browsers (PC, Mac, iOS, Android)
- ▶ CJP will be providing the first year of training/testing free of charge

To Enroll: Contact us at cjpcybersecurity@cjp.org

InteProIQ: Awareness Training Topics



INFOSEC 101

Defining your role
Defending your information



CONNECTIVITY

Information Sharing
Secure/Insecure Connections



SOCIAL ENGINEERING

Identifying Types of Scams
Maintaining a Safe
Environment



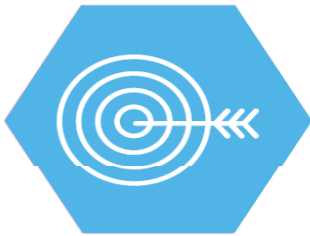
PASSWORDS

Password Management
Encryption



DEVICES

Storage, Printers, Fax
Machines
Discarding Old Equipment



MALICIOUS ATTACKS

Identifying Types of Attacks
Taking Proactive Actions



INCIDENT REPORTING

Common Misconceptions
Recognizing and Reporting

Good Password Hygiene

- ▶ **Avoid reusing passwords** – Use different passwords for Work vs. Personal
- ▶ **Use ‘passphrases’ instead of ‘passwords’**
 - Use complexity in your passphrases Ex: 3BlindMice#C#HowTheyRun4it!
- ▶ **Enable two-factor authentication**
- ▶ **Protect your password list** – if you must have a list
 - Use a cryptic list . . . like a ‘hint’ list
- ▶ **Consider a password manager**

Data Security

- ▶ **Your agency/organization data is their data**
- ▶ **Be extra careful sharing any data – check the email**
- ▶ **Encrypt when sharing any data with an external party**
- ▶ **Back up your data**
- ▶ **Lock your computer anytime you leave your desk**
- ▶ **When in doubt, ask your Manager or head of IT**



Protect Yourself At Home

- ▶ **Turn on automatic updates for home PC's** – system and anti-malware software
- ▶ **Secure your home IoT devices** – change default passwords
- ▶ **Be careful with your use wireless** – at home and public Wi-Fi
- ▶ **Back up your data**
- ▶ **Store sensitive data offline**
- ▶ **Cover your webcams**



Be a Cyber Partner

- ▶ Everyone must be vigilant
- ▶ When in doubt don't click
- ▶ Enroll in InteProIQ Awareness Training
- ▶ Questions about phishing or a policy ask your manager or IT



Top 10 Cyber Tips

TIP 1

GET WISE TO
**Phishing
Scams**



TIP 2

PROTECT
**Sensitive
Data**



TIP 3

PROTECT ALL YOUR
Devices



TIP 4

PRACTICE GOOD
**Password
Management**



TIP 5

BACK UP YOUR
Data



TIP 6

BE WARY OF
**Wi-Fi
Networks**



TIP 9

ENABLE
**Two-Factor
Authentication
(2FA)**



TIP 10

BEWARE THE
Internet of Things



TIP 7

PUT YOUR
**Credit
on Ice**



TIP 8



DON'T BE TOO
Social

Cyber Tips

Keep yourself and your
family cyber safe.

Question & Answer



For More Cyber Information

TedP@cjp.org

EvanP@cjp.org

Nancy.Viner@gmail.com

CommunalSecurity@cjp.org

To Enroll in InteProIQ Awareness Training:

cjpcybersecurity@cjp.org