PROTECTING THE CONSUMER'S FUTURE
NAHU
National Association of Health Underwriters
AMERICA'S BENEFITS SPECIALISTS

5 Steps to Protecting Your Organization From Cyber Attacks

Presented by

Jack McGrath
President
Digitec Interactive

July 2017

This compliance corner is sponsored by the LPRT Committee

The View from the Top is Great….So are the benefits of being there!

Find out more on NAHU's website, search "LPRT"

LEADING PRODUCERS ROUND TABLE

NAHU

Encouraging excellence in health and benefits insurance professionals since 1942

Sponsored by LPRT

Circle of Excellence

SOARING EAGLE

NAHU Leading Producers Round Table

What's the BIG deal?

- Profound Testimonial about YOU
- Distinguished
- Knowledgeable
- Successful
- The ELITE in your profession
- Motivation …

QUESTIONS?

You may ask your question in the questions box at any time. Any questions that we do not answer during the webinar will be posted on the compliance corner webpage in the coming weeks.

The information herein should not be construed as legal or tax advice in any way. Regulations, guidance and legal opinions continue to change. The preparer has gathered public information and has attempted to present it in an easily readable and understandable format. Situations vary, technical corrections and future guidance may vary from what is discussed in the presentation.

This is meant for informational content only. The presenter makes no warranty of any kind concerning this information. You should seek the advice of your attorney or tax consultant for additional or specific information.

This presentation is not to be duplicated or distributed.

TODAY’S PRESENTER

Jack McGrath

President of Digitec Interactive

- Digitec has been designing and developing interactive learning since the 1990s and is nationally recognized for eLearning course design.
- Digitec has delivered **cyber security** training for organizations including ISACA, GoPro, Cisco Systems, NetDefense Pro and others.
- Digitec also designs and delivers online compliance training.

WHY?

- The latest hacking scams are targeting agencies/brokers, human resource departments, providers and carriers. All the people that we work with on a daily basis.
- Social media and job search sites are also being targeted.

WHY?

- Who has all the information needed to steal an identity—name, address, DOB, SSN
- The targeted companies don't necessarily have training systems in place to protect data
- Don't become one of the statistics that will be mentioned in this presentation

AGENDA – TOP 5

1. Think before you click - Avoiding phishing scams and ransomware.
2. Be a human firewall - Spotting and thwarting social engineering scams and identity scams
3. Reinforce password security
4. Be afraid of USB drives and public connections
5. Do continual employee security awareness training

Statistics

- 62% of cyberattacks are targeted at small and medium sized companies
- 2016 saw a 752% hike in new ransomware families which resulted in $1 billion in losses for enterprises worldwide, according to Trend Micro
- 80% of cyberattacks are caused by your employees
- A 2012 study by the National Cyber Security Alliance, found that 60 % of small firms go out of business within six months of a data breach.

DON'T LET THIS
BE YOU!

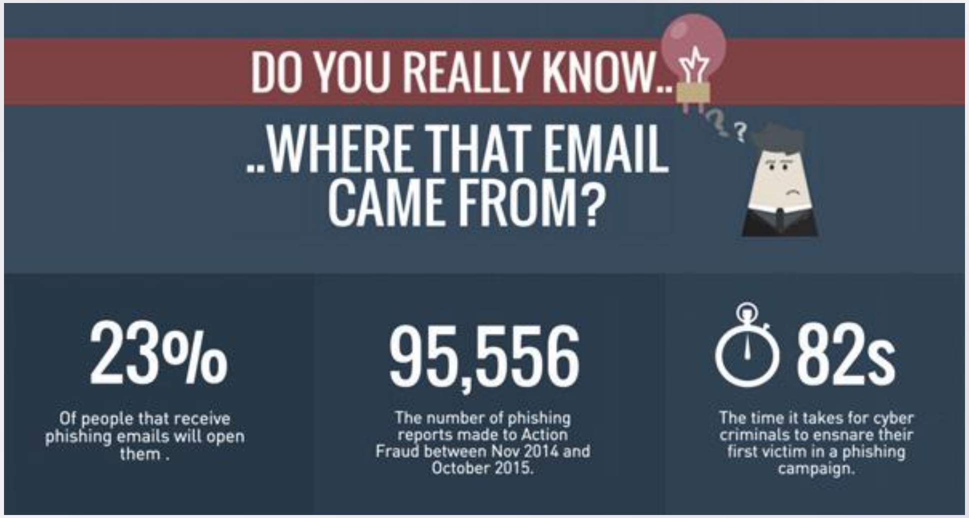
References:

- Bruemmer, Michael. (2014) Experian. Reported in USA Today
- Trend Micro
- Timothy Francis, "Hacked: The Implications of a Cyber Breach," Travelers Insurance
- National Cyber Security Alliance, (2012) America's Small Businesses Must Take Online Security More Seriously

1. Think before you click

What is phishing?

- Attempt to gain personal information from an individual by pretending to be a reputable organization.
- Most often this occurs though email but sometimes through text messaging as well.



DO YOU REALLY KNOW..

..WHERE THAT EMAIL CAME FROM?

23%

Of people that receive phishing emails will open them .

95,556

The number of phishing reports made to Action Fraud between Nov 2014 and October 2015.

82s

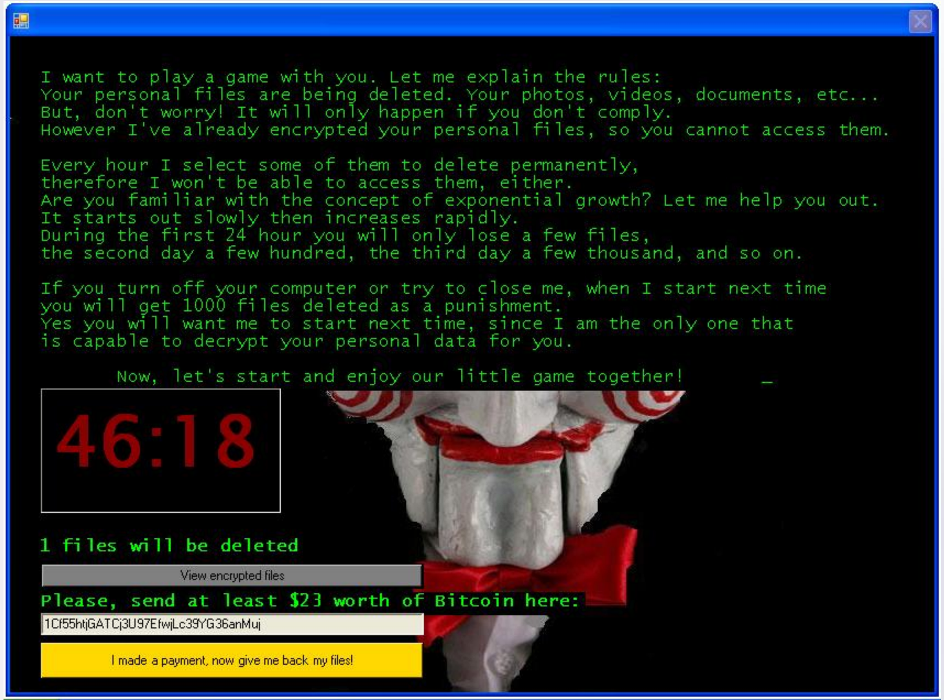
The time it takes for cyber criminals to ensnare their first victim in a phishing campaign.

A person may receive an email from someone pretending to be from the bank for example, suggesting the account has been fraudulently accessed. They are asked to verify the account details to protect your account. When verified, the account details and personal information is sent.

1. Think before you click

What is ransomware?

- Accesses information on your network
- Encrypts your data
- Demands a fee to release your data.
- You are then locked out of your data until you pay their fee for release.



```
I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

        Now, let's start and enjoy our little game together!

46:18

1 files will be deleted
```

```
Please, send at least $23 worth of Bitcoin here:
1Cf55htjGATCj3U97EfwjLc39YG36anMuj
```

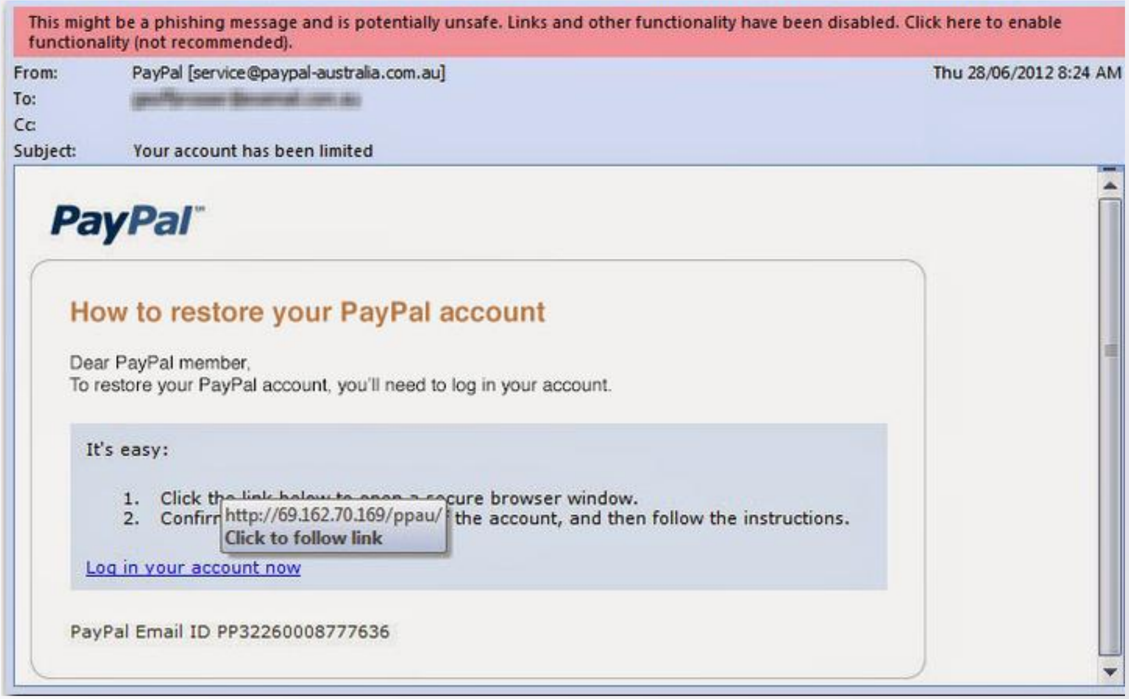
Typically, the victim is told to pay the ransom amount in bitcoin. Bitcoin is a type of digital currency in which encryption techniques are used to verify the transfer of funds

DO NOT PAY. Contact the authorities.

1. Think before you click

Be skeptical. Is this a phishing scam?

- Are there any red flags in this email?
- Does it look legitimate?
- How can you tell?



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] Thu 28/06/2012 8:24 AM
To: [redacted]
Cc:
Subject: Your account has been limited

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click th cure browser window.
2. Confirr the account, and then follow the instructions.

Log in your account now

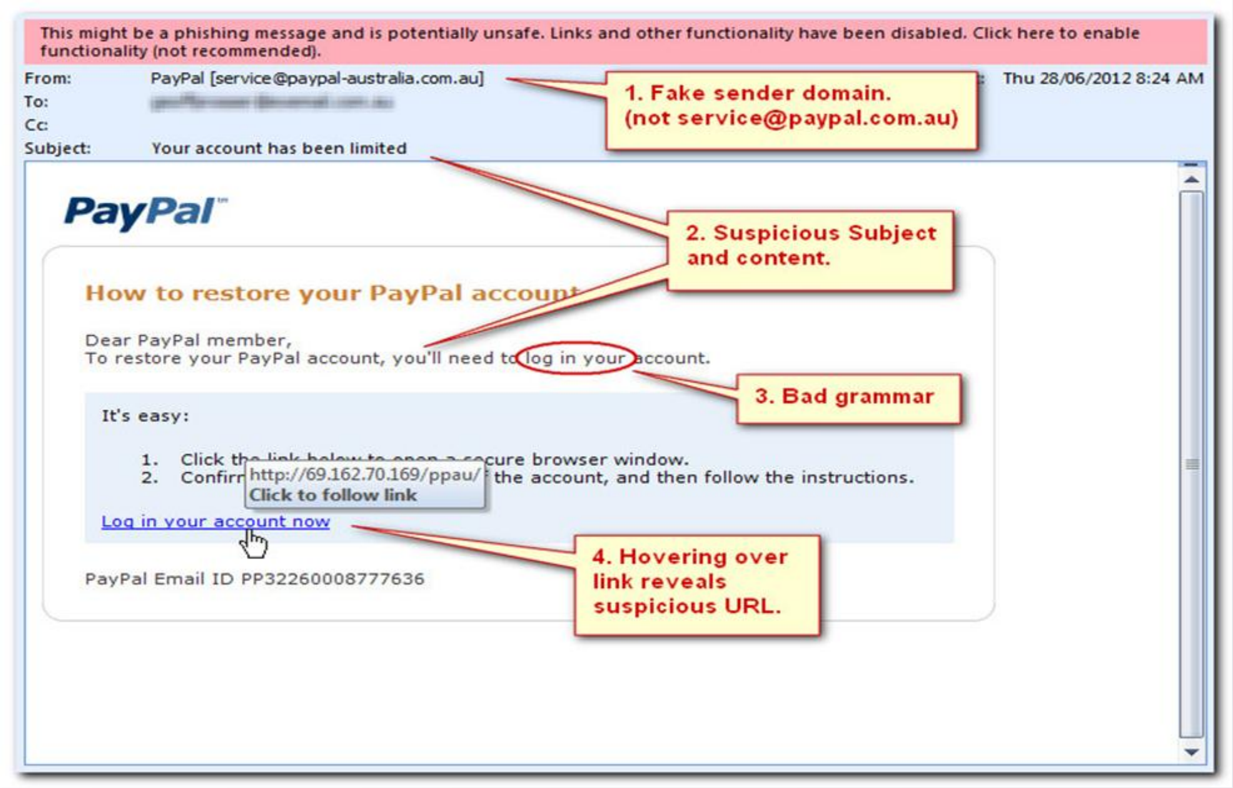
PayPal Email ID PP32260008777636

1. Think before you click

What do you look for?

- Fake sender domain
- Suspicious subject and content
- Bad grammar
- Suspicious URL

ALERT
HR scams involving job postings



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]

To: [redacted]

Cc:

Subject: Your account has been limited

: Thu 28/06/2012 8:24 AM

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.

Log in your account now

PayPal Email ID PP32260008777636

1. Fake sender domain. (not service@paypal.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

2. Be a Human Firewall

What is a social engineering scam?

- Someone plays the part of a person of authority at a company
- They attempt to obtain sensitive information from someone within the company.

Hi Amy,
This is Joe, from IT...I'm working from home today...

A criminal pretends to be a coworker or a level of upper management. They call ***or email*** *asking for a password reset or some other piece of sensitive data.*

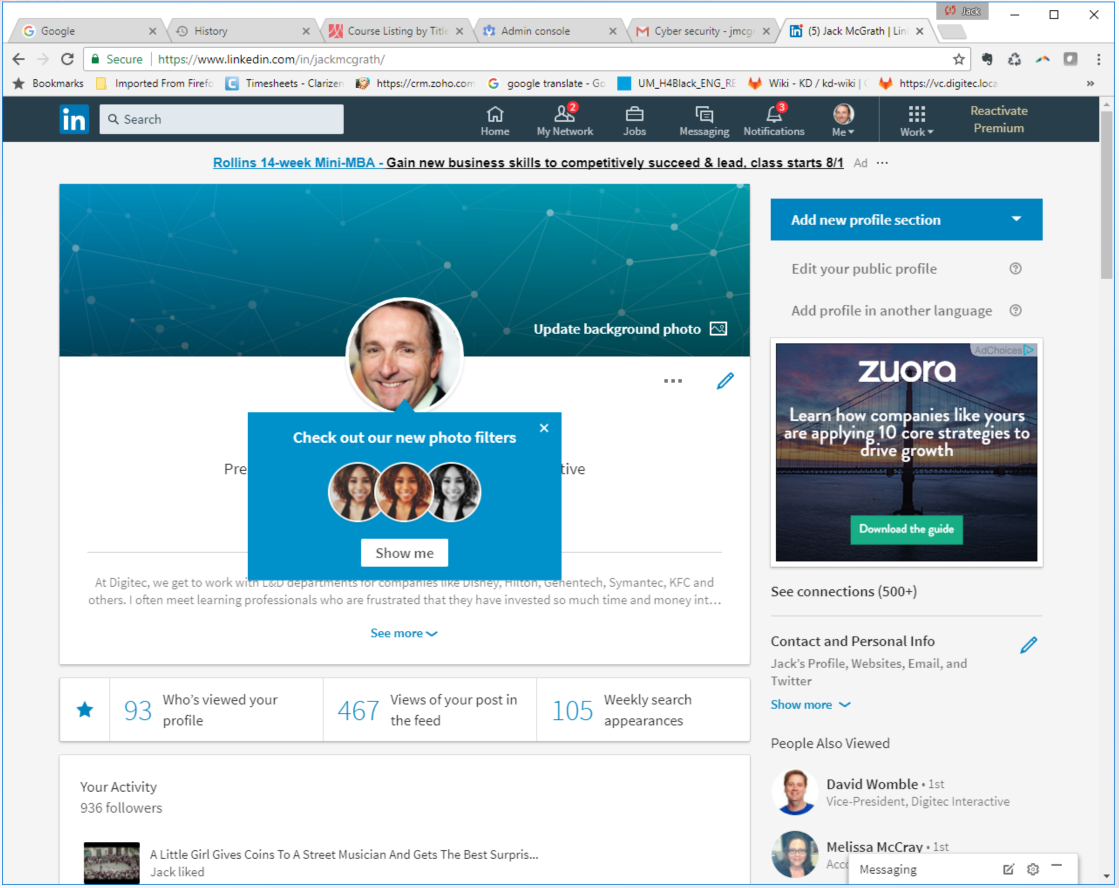
They seem official, using the correct name and email of the person they are imitating.

The employee complies by either providing company information or resetting passwords. By doing so, they have just given a criminal access to the data.

2. Be a Human Firewall

Social media mining

LinkedIn, and other popular social networking sites, are additional sources for these types of cyber attacks.



Rollins 14-week Mini-MBA - Gain new business skills to competitively succeed & lead, class starts 8/1 Ad

Check out our new photo filters

Learn how companies like yours are applying 10 core strategies to drive growth

At Digitec, we get to work with L&D departments for companies like Disney, Hilton, Genentech, Symantec, KFC and others. I often meet learning professionals who are frustrated that they have invested so much time and money int...

93 Who's viewed your profile | 467 Views of your post in the feed | 105 Weekly search appearances

Contact and Personal Info
Jack's Profile, Websites, Email, and Twitter

Your Activity
936 followers

A Little Girl Gives Coins To A Street Musician And Gets The Best Surpris...
Jack liked

People Also Viewed
David Womble • 1st
Vice-President, Digitec Interactive
Melissa McCray • 1st

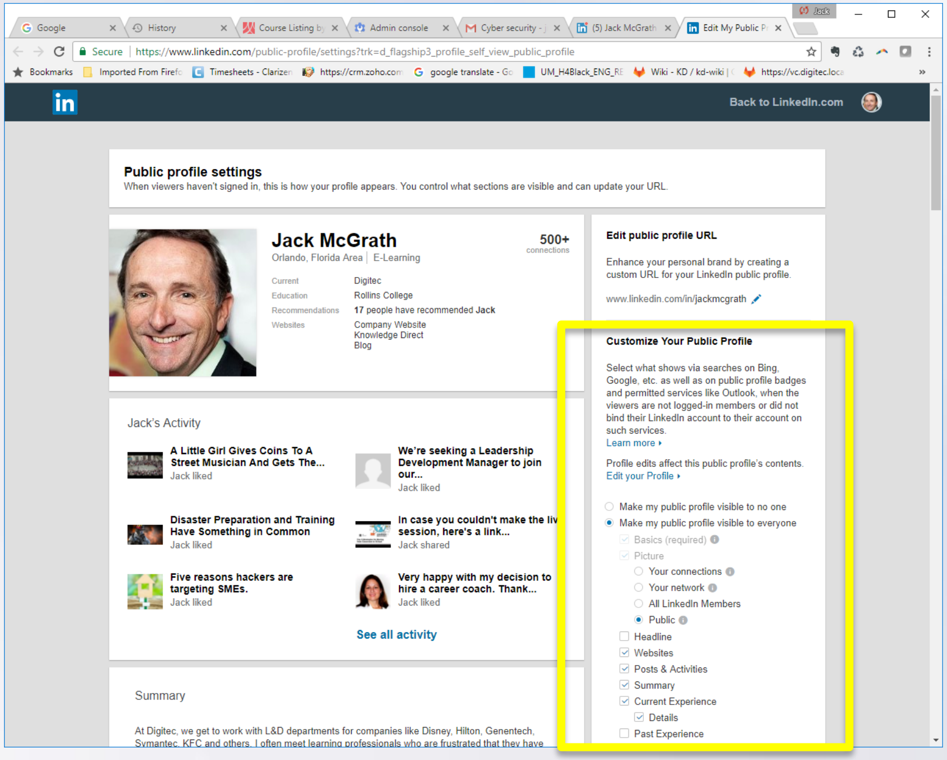
The FBI recently completed a study showing a 270% increase of identified victims, with over $2.3 B in losses due to these scams and activities.

Reference:
Krebson security, (2016) “FBI: $2.3 Billion Lost to CEO Email Scams“

2. Be a Human Firewall

Think like a "firewall"

- Scrutinize all incoming requests
- Verify (**Is Joe from IT working from home today?)**
- Confirm the information before taking action
- Be wary how much information you share on social media



Public profile settings

When viewers haven't signed in, this is how your profile appears. You control what sections are visible and can update your URL.

Jack McGrath

Orlando, Florida Area | E-Learning

500+ connections

Current	Digitec
Education	Rollins College
Recommendations	17 people have recommended Jack
Websites	Company Website Knowledge Direct Blog

Jack's Activity

A Little Girl Gives Coins To A Street Musician And Gets The...
Jack liked

We're seeking a Leadership Development Manager to join our...
Jack liked

Disaster Preparation and Training Have Something in Common
Jack liked

In case you couldn't make the liv session, here's a link...
Jack shared

Five reasons hackers are targeting SMEs.
Jack liked

Very happy with my decision to hire a career coach. Thank...
Jack liked

See all activity

Summary

At Digitec, we get to work with L&D departments for companies like Disney, Hilton, Genentech, Symantec, KFC and others. I often meet learning professionals who are frustrated that they have

Edit public profile URL

Enhance your personal brand by creating a custom URL for your LinkedIn public profile.

www.linkedin.com/in/jackmcgrath

Customize Your Public Profile

Select what shows via searches on Bing, Google, etc. as well as on public profile badges and permitted services like Outlook, when the viewers are not logged-in members or did not bind their LinkedIn account to their account on such services.
Learn more ›

Profile edits affect this public profile's contents.
Edit your Profile ›

○ Make my public profile visible to no one
● Make my public profile visible to everyone
- ☑ Basics (required)
- ☑ Picture
  - ○ Your connections
  - ○ Your network
  - ○ All LinkedIn Members
  - ● Public
- □ Headline
- ☑ Websites
- ☑ Posts & Activities
- ☑ Summary
- ☑ Current Experience
  - ☑ Details
- □ Past Experience

3. Reinforce password security

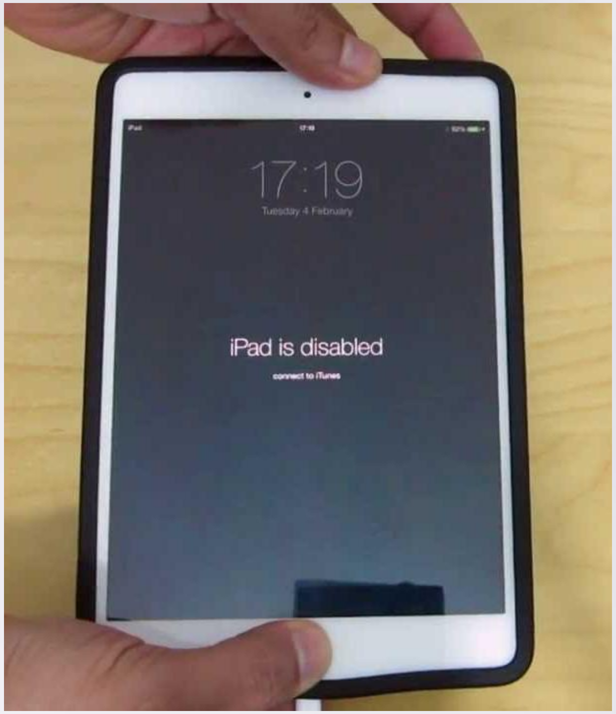
Most hacked passwords of 2016

1. 123456
2. Password
3. 12345678
4. Qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars

Source: The Guardian, "How to create the perfect password" 2016)

3. Reinforce password security

- Check your existing password
- Make it long
- Passphrase not password
- Use special characters
- Maintain digital hygiene
- Lock your computer and tablet



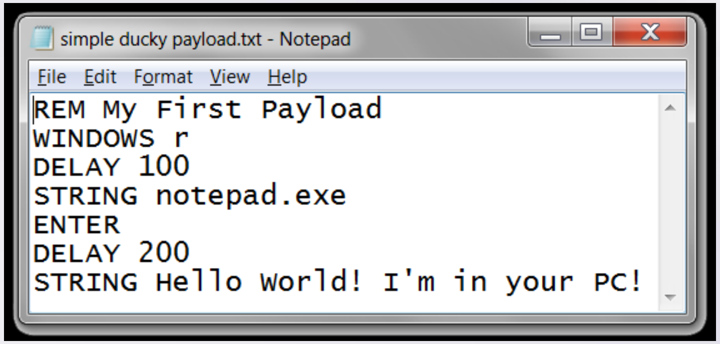
Consider a password manager

A password manager is a software application or hardware that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password: a single, ideally very strong password which grants the user access to their entire password database.

4. Be afraid of USB drives and public connections

USB drives are sources of malware

- Can introduce threats such as the Stuxnet malicious computer worm
- Antivirus is a must! Make sure you have Norton or Symantec running and updated


simple ducky payload.txt - Notepad
File Edit Format View Help

```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

"If someone plugs an infected USB drive into their home computer they could inadvertently upload a virus and potentially cripple the machine. And if they connect to their office network the worm can upload and replicate itself on the network."

-Norton 2016

4. Be afraid of USB drives and public connections

Wifi insecurities and mobile devices

- Free airport and hotel wifi is not safe. Use your phone as a hotspot
- For mobile devices, use a ‘kill’ program, so if a phone or tablet is lost or stolen, the data can be quickly and remotely wiped.

5. Do continual employee security awareness training

Cybersecurity training

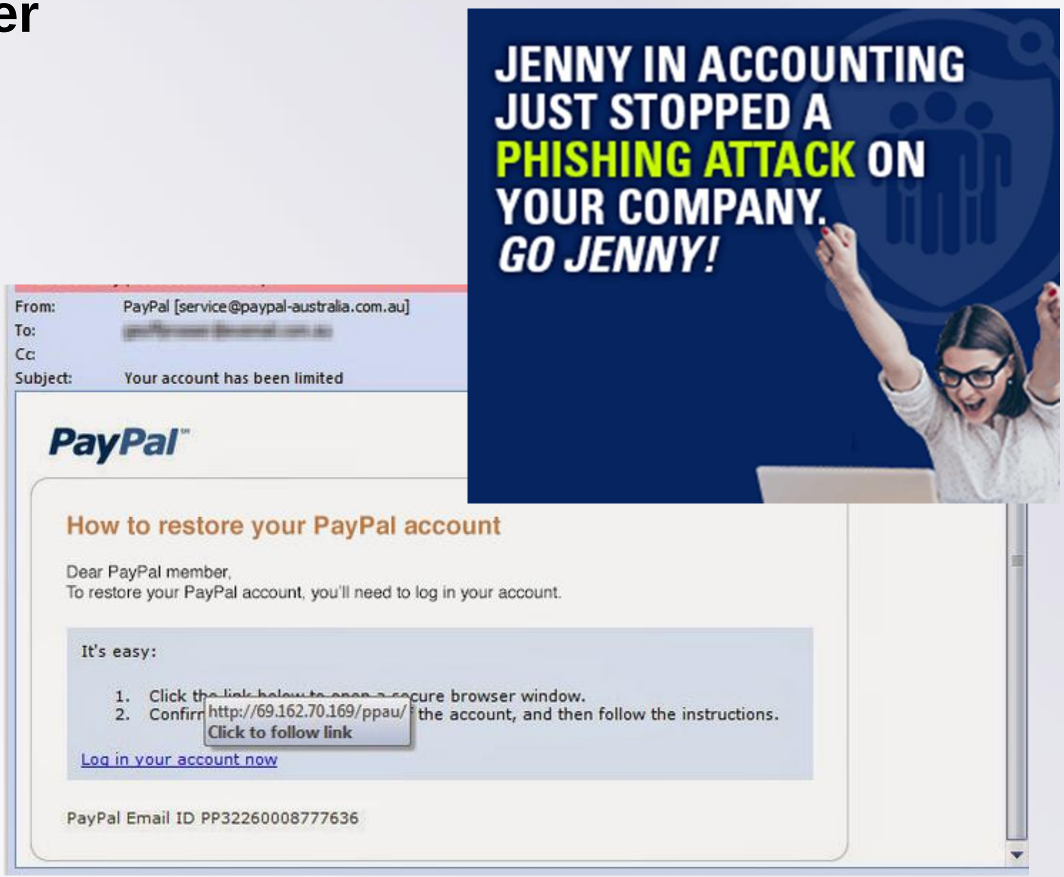
- The best defense against an attack is employee awareness
- IT departments can't be everywhere at once, and need an informed workplace to help protect the assets
- Some states have cyber security laws that require training, with potential fines

Employees result in 80% of all cybersecurity issues.

5. Do continual employee security awareness training

Provide ongoing cyber security training

- Startup course
- Monthly updates
- Phishing attack simulations
- Dashboard tracking



JENNY IN ACCOUNTING JUST STOPPED A PHISHING ATTACK ON YOUR COMPANY.
GO JENNY!

From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click th cure browser window.
2. Confirr the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

RECAP

1. Think before you click - Avoiding phishing scams and ransomware.
2. Be a human firewall - Spotting and thwarting social engineering scams and identity scams
3. Reinforce password security
4. Be afraid of USB drives and public connections
5. Do continual employee security awareness training

CONTACT

Jack McGrath
Digitec Interactive

6000 Metrowest Blvd
Suite 200
Orlando, FL 32835
(407) 299-1800

www.netdefensepro.com
info@netdefensepro.com

NETDEFENSE PRO
CYBERSECURITY TRAINING

Contact us for a free 10 day trial

Purchase before 8/31/17 and earn 50% off for 2017

@netdefensepro

facebook.com/NetDefensePro/

THANK YOU FOR ATTENDING

Compliance Corner Resources

- The new *Compliance Cornered* Blog
- Archived, topical webinars
- Resource pages, documents, and FAQs
- Ask a question to legislative@nahu.org