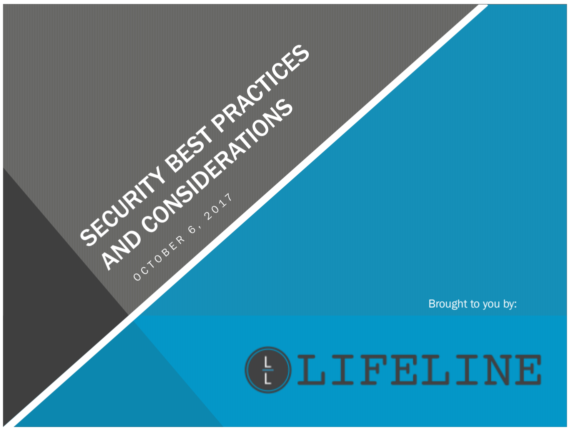
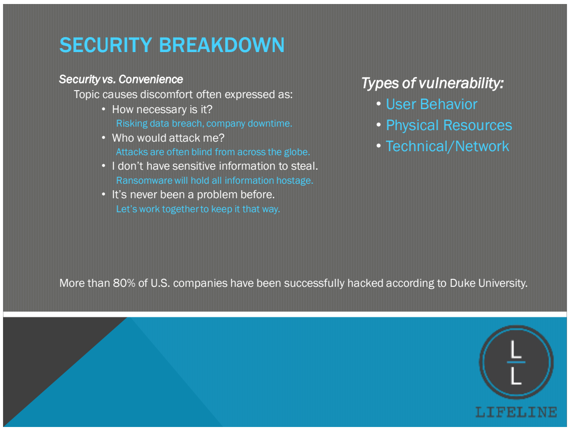


SECURITY BEST PRACTICES AND CONSIDERATIONS

OCTOBER 6, 2017

Brought to you by:

LIFELINE



SECURITY BREAKDOWN

Security vs. Convenience

Topic causes discomfort often expressed as:

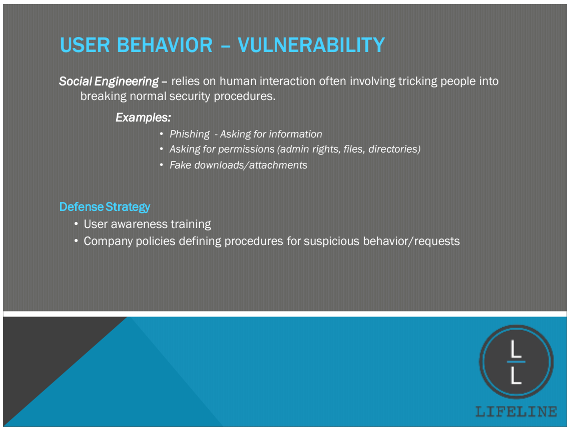
- How necessary is it?
  Risking data breach, company downtime.
- Who would attack me?
  Attacks are often blind from across the globe.
- I don't have sensitive information to steal.
  Ransomware will hold all information hostage.
- It's never been a problem before.
  Let's work together to keep it that way.

Types of vulnerability:

- User Behavior
- Physical Resources
- Technical/Network

More than 80% of U.S. companies have been successfully hacked according to Duke University.

LIFELINE



USER BEHAVIOR – VULNERABILITY

Social Engineering – relies on human interaction often involving tricking people into breaking normal security procedures.

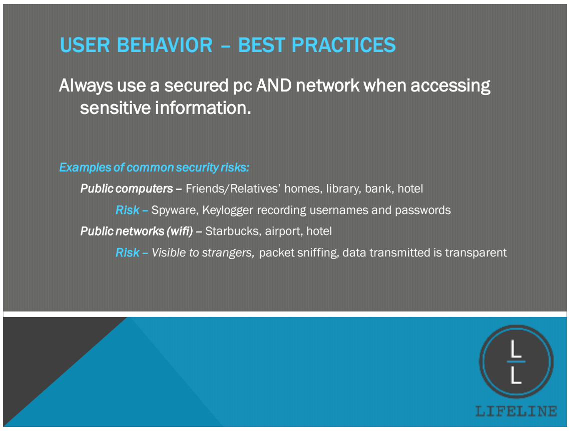
Examples:

- *Phishing - Asking for information*
- *Asking for permissions (admin rights, files, directories)*
- *Fake downloads/attachments*

Defense Strategy

- User awareness training
- Company policies defining procedures for suspicious behavior/requests

LIFELINE



USER BEHAVIOR – BEST PRACTICES

Always use a secured pc AND network when accessing sensitive information.

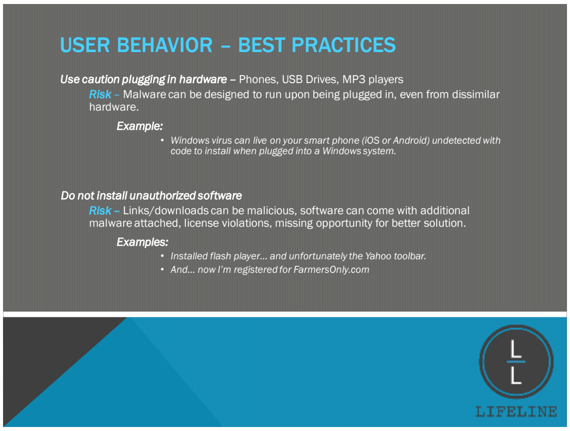
Examples of common security risks:

Public computers **–** Friends/Relatives' homes, library, bank, hotel

Risk – Spyware, Keylogger recording usernames and passwords

Public networks (wifi) **–** Starbucks, airport, hotel

Risk – Visible to strangers, packet sniffing, data transmitted is transparent



USER BEHAVIOR – BEST PRACTICES

Use caution plugging in hardware **–** Phones, USB Drives, MP3 players

Risk – Malware can be designed to run upon being plugged in, even from dissimilar hardware.

Example:

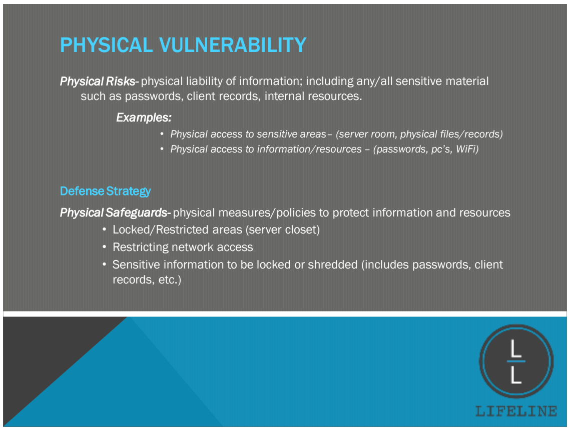
- *Windows virus can live on your smart phone (iOS or Android) undetected with code to install when plugged into a Windows system.*

Do not install unauthorized software

Risk – Links/downloads can be malicious, software can come with additional malware attached, license violations, missing opportunity for better solution.

Examples:

- *Installed flash player… and unfortunately the Yahoo toolbar.*
- *And… now I'm registered for FarmersOnly.com*



PHYSICAL VULNERABILITY

Physical Risks- physical liability of information; including any/all sensitive material such as passwords, client records, internal resources.

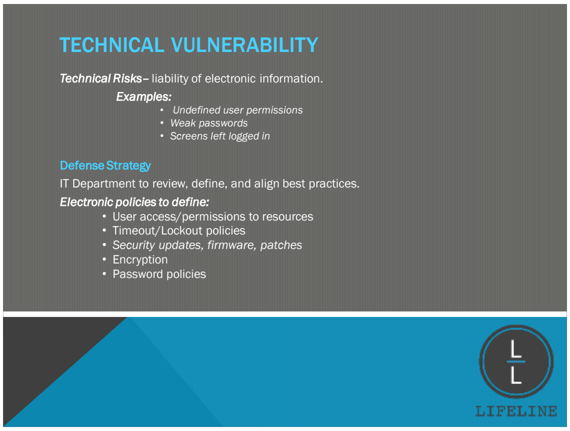
Examples:

- *Physical access to sensitive areas – (server room, physical files/records)*
- *Physical access to information/resources – (passwords, pc's, WiFi)*

Defense Strategy

Physical Safeguards- physical measures/policies to protect information and resources

- Locked/Restricted areas (server closet)
- Restricting network access
- Sensitive information to be locked or shredded (includes passwords, client records, etc.)



TECHNICAL VULNERABILITY

Technical Risks – liability of electronic information.

Examples:

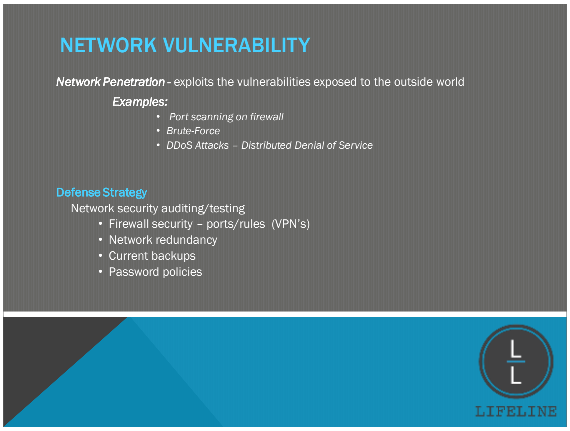
- *Undefined user permissions*
- *Weak passwords*
- *Screens left logged in*

Defense Strategy

IT Department to review, define, and align best practices.

Electronic policies to define:

- User access/permissions to resources
- Timeout/Lockout policies
- *Security updates, firmware, patches*
- Encryption
- Password policies



NETWORK VULNERABILITY

Network Penetration - exploits the vulnerabilities exposed to the outside world

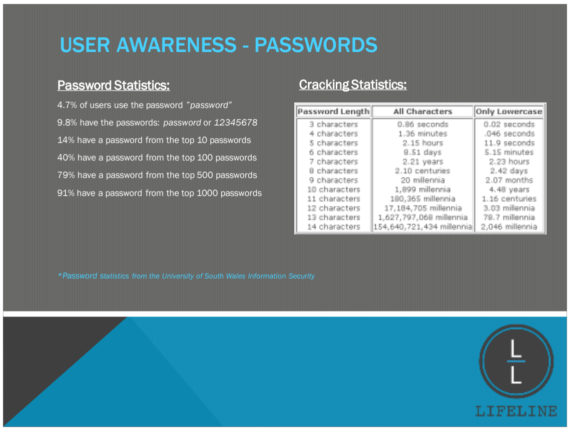
Examples:

- *Port scanning on firewall*
- *Brute-Force*
- *DDoS Attacks – Distributed Denial of Service*

Defense Strategy

Network security auditing/testing

- Firewall security – ports/rules (VPN's)
- Network redundancy
- Current backups
- Password policies



USER AWARENESS - PASSWORDS

Password Statistics:

4.7% of users use the password *"password"*

9.8% have the passwords: *password* or *12345678*

14% have a password from the top 10 passwords

40% have a password from the top 100 passwords

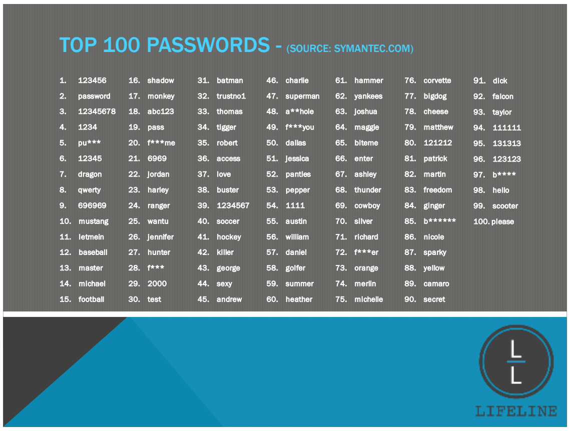
79% have a password from the top 500 passwords

91% have a password from the top 1000 passwords

Cracking Statistics:

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

**Password statistics from the University of South Wales Information Security*

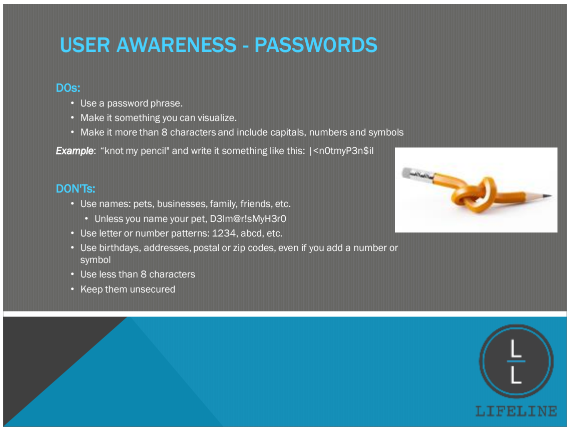


TOP 100 PASSWORDS - (SOURCE: SYMANTEC.COM)

1. 123456
2. password
3. 12345678
4. 1234
5. pu***
6. 12345
7. dragon
8. qwerty
9. 696969
10. mustang
11. letmein
12. baseball
13. master
14. michael
15. football
16. shadow
17. monkey
18. abc123
19. pass
20. f***me
21. 6969
22. jordan
23. harley
24. ranger
25. wantu
26. jennifer
27. hunter
28. f***
29. 2000
30. test
31. batman
32. trustno1
33. thomas
34. tigger
35. robert
36. access
37. love
38. buster
39. 1234567
40. soccer
41. hockey
42. killer
43. george
44. sexy
45. andrew
46. charlie
47. superman
48. a**hole
49. f***you
50. dallas
51. jessica
52. panties
53. pepper
54. 1111
55. austin
56. william
57. daniel
58. golfer
59. summer
60. heather
61. hammer
62. yankees
63. joshua
64. maggie
65. biteme
66. enter
67. ashley
68. thunder
69. cowboy
70. silver
71. richard
72. f***er
73. orange
74. merlin
75. michelle
76. corvette
77. bigdog
78. cheese
79. matthew
80. 121212
81. patrick
82. martin
83. freedom
84. ginger
85. b******
86. nicole
87. sparky
88. yellow
89. camaro
90. secret
91. dick
92. falcon
93. taylor
94. 111111
95. 131313
96. 123123
97. b****
98. hello
99. scooter
100. please

USE STRONG PASSWORDS

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."



USER AWARENESS - PASSWORDS

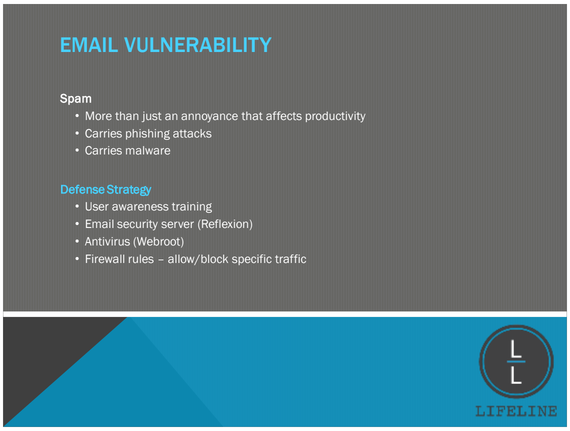
DOs:

- Use a password phrase.
- Make it something you can visualize.
- Make it more than 8 characters and include capitals, numbers and symbols

Example: "knot my pencil" and write it something like this: |<n0tmyP3n$il

DON'Ts:

- Use names: pets, businesses, family, friends, etc.
  - Unless you name your pet, D3lm@r!sMyH3r0
- Use letter or number patterns: 1234, abcd, etc.
- Use birthdays, addresses, postal or zip codes, even if you add a number or symbol
- Use less than 8 characters
- Keep them unsecured



EMAIL VULNERABILITY

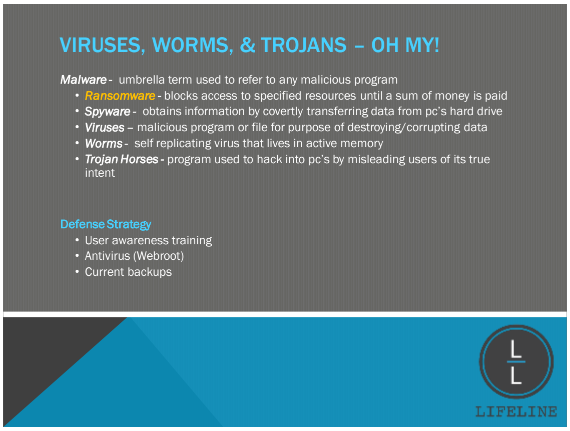
Spam

- More than just an annoyance that affects productivity
- Carries phishing attacks
- Carries malware

Defense Strategy

- User awareness training
- Email security server (Reflexion)
- Antivirus (Webroot)
- Firewall rules – allow/block specific traffic

LIFELINE



VIRUSES, WORMS, & TROJANS – OH MY!

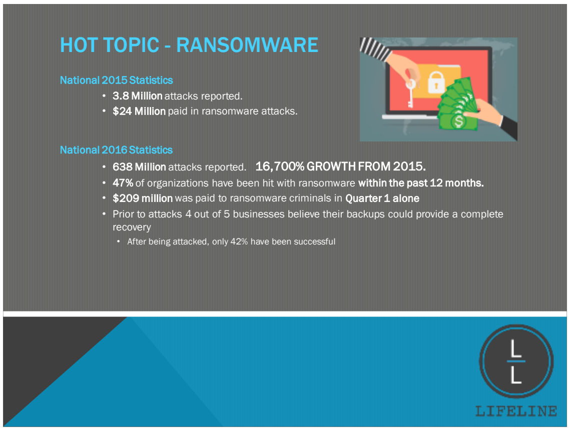
Malware - umbrella term used to refer to any malicious program

- *Ransomware* - blocks access to specified resources until a sum of money is paid
- ***Spyware*** - obtains information by covertly transferring data from pc's hard drive
- ***Viruses*** – malicious program or file for purpose of destroying/corrupting data
- ***Worms*** - self replicating virus that lives in active memory
- ***Trojan Horses*** - program used to hack into pc's by misleading users of its true intent

Defense Strategy

- User awareness training
- Antivirus (Webroot)
- Current backups

LIFELINE



HOT TOPIC - RANSOMWARE

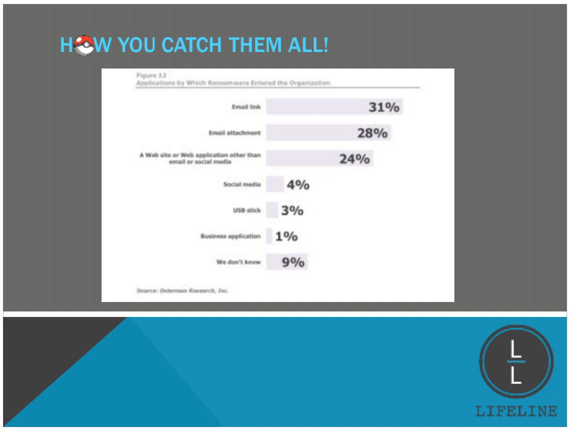
National 2015 Statistics

- **3.8 Million** attacks reported.
- **$24 Million** paid in ransomware attacks.

National 2016 Statistics

- **638 Million** attacks reported. 16,700% GROWTH FROM 2015.
- **47%** of organizations have been hit with ransomware **within the past 12 months.**
- **$209 million** was paid to ransomware criminals in **Quarter 1 alone**
- Prior to attacks 4 out of 5 businesses believe their backups could provide a complete recovery
  - After being attacked, only 42% have been successful

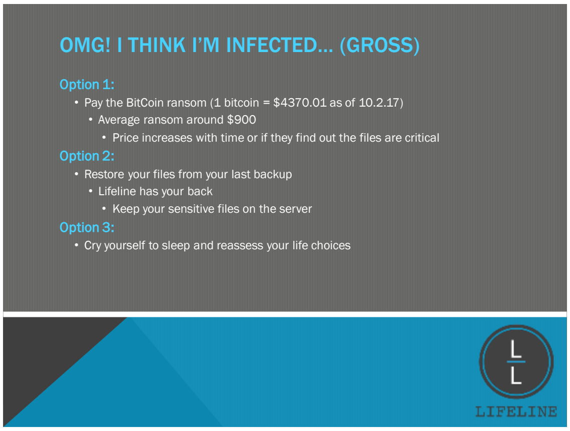
LIFELINE



H◓W YOU CATCH THEM ALL!

Figure 12
Applications by Which Ransomware Entered the Organization

Source: Osterman Research, Inc.

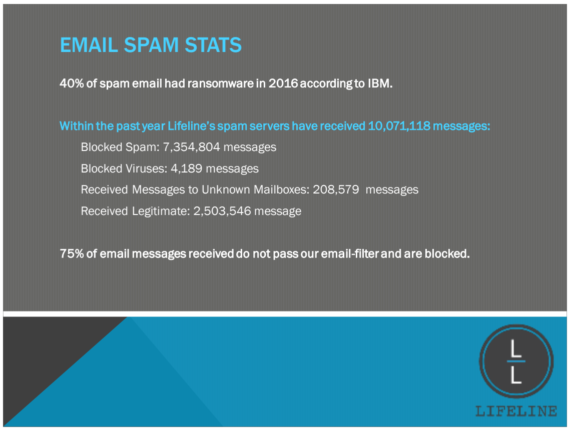


OMG! I THINK I'M INFECTED… (GROSS)

Option 1:
- Pay the BitCoin ransom (1 bitcoin = $4370.01 as of 10.2.17)
  - Average ransom around $900
    - Price increases with time or if they find out the files are critical

Option 2:
- Restore your files from your last backup
  - Lifeline has your back
    - Keep your sensitive files on the server

Option 3:
- Cry yourself to sleep and reassess your life choices



EMAIL SPAM STATS

40% of spam email had ransomware in 2016 according to IBM.

Within the past year Lifeline's spam servers have received 10,071,118 messages:

Blocked Spam: 7,354,804 messages

Blocked Viruses: 4,189 messages

Received Messages to Unknown Mailboxes: 208,579 messages

Received Legitimate: 2,503,546 message

75% of email messages received do not pass our email-filter and are blocked.

WHOA! DON'T OPEN THAT EMAIL

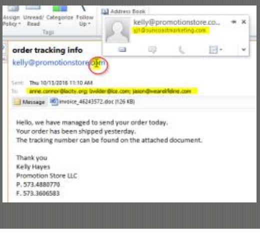
User considerations

- Do you know the sender?
- Are you expecting the email?
- Does the email seem legitimate?

Protect yourself

- Never enter personal information in a pop-up.
- Call/Confirm with the sender.
- Analyze links and attachments.
- Verify the email address. Use the hover trick or check the Reflexion summary at the bottom of the email.

VERIFY SENDER - HOVER TRICK



kelly@promotionstore.co...
yj1@suncoastmarketing.com

order tracking info
kelly@promotionstore.com

Sent: Thu 10/13/2016 11:10 AM
To: anne.connor@lacity.org; bvilder@lce.com; jason@wearelifeline.com

Message invoice_46243572.doc (126 KB)

Hello, we have managed to send your order today.
Your order has been shipped yesterday.
The tracking number can be found on the attached document.

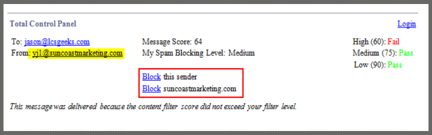
Thank you
Kelly Hayes
Promotion Store LLC
P. 573.4880770
F. 573.3606583

- Hover your cursor over the sender's address. Notice the actual address is different.
- Bonus Red Flag:
  - Also notice the other recipients on this email. "My Order Info" was sent to several recipients that I don't recognize.

VERIFY SENDER – REFLEXION SUMMARY

Second method of verifying sender.

- Use the Reflexion Summary at the bottom of external emails.



Total Control Panel Login

To: jason@lcsgeeks.com
From: yj1@suncoastmarketing.com

Message Score: 64
My Spam Blocking Level: Medium

High (60): Fail
Medium (75): Pass
Low (90): Pass

Block this sender
Block suncoastmarketing.com

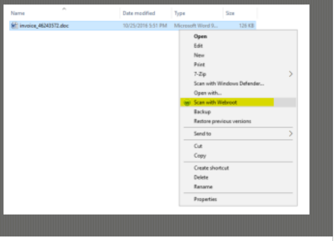
This message was delivered because the content filter score did not exceed your filter level.

Block the sender or the entire domain

ANALYZE EMAILS ATTACHMENTS

Scan potentially trusted attachments before opening.

- Download attachment > Right-Click> Scan with Webroot.
- *NOTE:* This is not failsafe. Scans work from Webroot's database and should be performed **AFTER** the user has identified the email as legitimate.



Name	Date modified	Type	Size
invoice_46243572.doc	10/25/2016 5:51 PM	Microsoft Word 9...	126 KB

LIFELINE

VIRUSES, WORMS, & TROJANS – OH MY!

Identifying a compromised PC

- Unusual slowness – often starting several minutes after startup
- Program pop-ups – often a fake antivirus program trying to scare users
- Browser pop-ups – unsolicited websites open, abundance of ads, blinking links
- Add/Remove programs showing bloatware – free arcade games, coupon finder
- General odd behavior – programs closing/stalling, new shortcuts, icons missing

Defense Strategy

- User awareness training
- Webroot
- IT Department manual cleanup

LIFELINE

WHAT SHOULD YOU DO

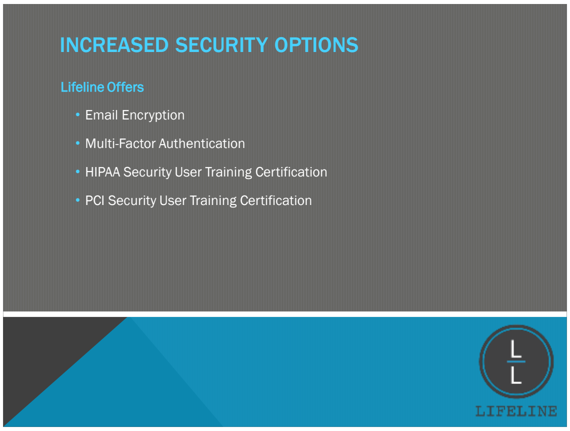
My pc's been infected

- Depending on severity/threat disconnect your pc from the network (power off)
- Change your password (very effective against pc hijacking)
- Contact Lifeline immediately
  - How many pc's are compromised?
  - What is affected?

My email account has been compromised

- Change your password immediately
- Check sent folder, and email any contacts that previous messages were bogus
- Contact Lifeline immediately

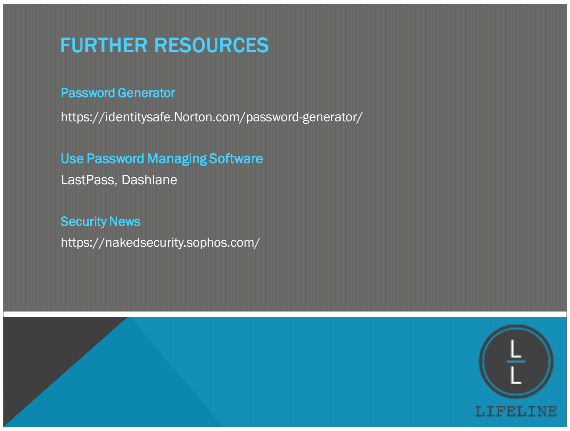
LIFELINE



INCREASED SECURITY OPTIONS

Lifeline Offers

- Email Encryption
- Multi-Factor Authentication
- HIPAA Security User Training Certification
- PCI Security User Training Certification



FURTHER RESOURCES

Password Generator

https://identitysafe.Norton.com/password-generator/

Use Password Managing Software

LastPass, Dashlane

Security News

https://nakedsecurity.sophos.com/