About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.
Agenda

Cybersecurity Landscape

Human Firewall

Putting it into Action
CYBERSECURITY LANDSCAPE

Persistent and ongoing brute force attacks on identities

Sophisticated spearphishing

Organizations targeted because of the work they do

Attacks targeting vendors
New security tools available to combat new threat types.

Organization's starting to ask about where to start in improving their cybersecurity.

68% of Nonprofits don’t have an Incident Response Plan

Breach response for a small to medium business is $149,000
QUESTION

• How confident do you feel in your knowledge about Cybersecurity?
  • Very Confident
  • Confident
  • Somewhat Confident
  • Not at all Confident
I know 15% of your password
Cybersecurity - Adversaries
It’s good to talk openly about cybersecurity.

Share your story and learn!

Your experience will help someone else.
• Supply Chain
• Staff at non-profits considered soft targets
• You may not consider your security important, but what about your donor list, board members, partners?
Contemporary Attack Examples

- Email Phishing
- Malware
- Social Engineering
Question (multiple choice)

• Have you experienced
  • Phishing emails
  • Virus / Malware / Ransomware
  • Social engineering
Phishing

Common attempts

How to identify

How to respond
Good Day,

The following payment notification has been sent to you by OnlineInvoices on behalf of Pioneer Credit Recovery. Please click the button below to view your details.

http://corpcatererscleveland.com/?24=UCPAUBYKV1CQUuQZCQi

$4,260.00
Invoice Id Number15067557933

Online Invoices
Easy online billing
New Device Detected...

Dear customer,

Click on the link below to update your devices.

Confirm your New Device
RE: How Are You Doing?

From: Joseph Weaver <jweavercpa@sbcglobal.net>
Phishing

1. Look at the email
2. Check for red flags
3. Ask someone or forward to your IT support provider
Email attachments
Malvertising
Spread via networks
Lon Ryall
4:27 PM

Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre
To:

Invoice INV-000993.7z
3.48 KB

Dear customer,

Here's invoice INV-000993 for USD 502.52.

[T] [http://allsexfinder.com/inv-00022.7z](http://allsexfinder.com/inv-00022.7z)
Click or tap to follow link.

Due on 9 Sept 2017.

View your bill online

From your online bill you can print a PDF, export a CSV, or create a free login and view your outstanding bills.

If you have any questions, please let us know.

Thanks,

Lon Ryall
Property Lagoon Limited
SECURE INVOICE

URGENT: Payment Overdue!!!

This document has been encrypted to protect your sensitive data
Please click “Enable Content” to view the invoice

This file is 100% virus-free
NO VIRUSES NO SPYWARE NO ADWARE
ASADA issues 12,000 pages of evidence against 34 Essendon players

October 17, 2014 - 5:35PM

Jon Pierik

Sports writer with The Age

The 34 Essendon players re-issued with show-cause notices have been given 350 pages of evidence alleging they were administered a banned peptide during the club's 2012 supplements program.
Dear Samsung SM-G930V user,

Wednesday, December 19, 2018

Congratulations Samsung SM-G930V user! You are one of the 10 users we personally selected to receive a $250 Costco Gift Card!

Costco Gift Card!

ACT NOW! 9 other Samsung users have received this invitation with only 5 prizes to be won.

You have **2 minutes 47 seconds** to answer the questions before someone else takes your spot. Good luck!

**Question 1 of 4:** Are you a regular Costco customer?

**YES**
MALWARE

1. Have antivirus and web filtering
2. Think before you click (or call)
3. Ensure systems are patched
Confidence Scheme
Exploits trust
Sense of urgency
To view the shared document, you are required to Login with your email address below:

Email Address: anonymous@contoso.com
Email Password: ***************
WARNING!

COMPUTER MAY BE AT RISK:

855-486-1800

Emergency Tech Support call immediately

System may have found (2) viruses that pose a serious threat
Rootkit.Siref.Spy ./ Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Call us now for support
855-486-1800
Social Engineering

1. Trick you into installing software
2. Trick you into entering credentials
3. Trick you into calling for “support”
OUR APPROACH TO CYBERSECURITY

NextGen Tools

IDENTITY  DATA  DEVICES  PERIMETER  WEB

SECURITY AWARENESS

SECURITY POLICY
Human Firewall
Devices

Identity

Security
You're capable of protecting your information

- Inventory
- Backup your data
Human Firewall

Patch and Update
- OS
- Firmware
- All devices
- Monthly
Enable and use Antivirus

• Only 40% effective (but 40% is better than 0%!)
Human Firewall

- Audit access to your Cloud Systems
- Be aware and honest
• Pick a good password
• Use a password Manager
• Enable MFA
SECURITY NONEXPERTS’ TOP ONLINE SAFETY PRACTICES VS SECURITY EXPERTS’ TOP ONLINE SAFETY PRACTICES

1. USE ANTIVIRUS SOFTWARE
2. USE STRONG PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY
4. ONLY VISIT WEBSITES THEY KNOW
5. DON’T SHARE PERSONAL INFORMATION

1. INSTALL SOFTWARE UPDATES
2. USE UNIQUE PASSWORDS
3. USE TWO-FACTOR AUTHENTICATION
4. USE STRONG PASSWORDS
5. USE A PASSWORD MANAGER
1. Backups
2. Updates
3. Antivirus
4. Audit Systems
5. Strong Passwords with MFA
Putting it into Action

Inventory systems
- Desktop
- Email
- Cloud Services
- Photos

Backup
- 2 locations
- You have control
Update your systems
• Operating System (Windows, Mac, iOS, Android)
• BIOS and Firmware Updates Quarterly
• Reboot weekly
Putting it into Action

Antivirus
- Windows Defender
- MacOS, XProtect

Web Filtering
- Cisco Umbrella
- Cloudflare
Putting it into Action

Get a password manager

• LastPass
• Dashlane

Pick a strong password

• Passphrase
  • One for your computer, one for the password manager
• Here are some guides
  • http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/
  • https://haveibeenpwned.com/Passwords
• Enable MFA
  • O365 MFA Enrollment Guide
  • Google Workspace MFA Guide
MFA IS EFFECTIVE

Account takeover prevention rates, by challenge type

- **Device-based challenges**
  - On-device prompt: 100% (Automated bot), 99% (Bulk phishing attack), 90% (Targeted attack)
  - SMS code: 100% (Automated bot), 96% (Bulk phishing attack), 76% (Targeted attack)
  - Security key: 100% (Automated bot), 100% (Bulk phishing attack), 100% (Targeted attack)

- **Knowledge-based challenges**
  - Secondary email address: 73% (Automated bot), 68% (Bulk phishing attack), 79% (Targeted attack)
  - Phone number: 100% (Automated bot), 26% (Bulk phishing attack), 50% (Targeted attack)
  - Last sign-in location: 10% (Automated bot), 100% (Bulk phishing attack), 100% (Targeted attack)

*95% confidence interval*
Pwned Passwords

Pwned Passwords are half a billion real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. Read more about how HIBP protects the privacy of searched passwords.

December2016

Oh no — pwned!
This password has been seen 7 times before

This password has previously appeared in a data breach and should never be used. If you’ve ever used it anywhere before, change it!
Security Check Up

Audit access to applications

- Facebook - https://www.facebook.com/help/799880743466869
- LinkedIn - https://www.linkedin.com/psettings/
Moving Forward

Security can be daunting, but it doesn't need to be overwhelming
Steps you can take

- Inventory and backup your data
- Update your computer (OS and Firmware)
- Make sure AV is installed
- Select a good password
  - Use a password manager
  - Turn on MFA
- Review System access and remove extra/unnecessary applications
- Schedule time for security
Schedule time for security

- Set a reminder for yourself
  - one week from today
- Have an accountability partner
  - monthly check in
Resources

• Community IT Webinar – https://www.communityit.com
• Stop Think Connect – https://www.stopthinkconnect.org