# Tech & Cyber Security: What the Board Needs to Know

THOUGHT LEADER
Erik Gudmundson,
Pegasus Technologies

PEGASUS
TECHNOLOGIES

## Board of Directors Workshop

*Join us virtually for nonprofit board governance best practices*

CHESTER COUNTY
community
FOUNDATION

Mark your calendars!
Mon. Oct. 18 2021

*Space is Limited. Register Early.*

*Register online at chescocf.org/ virtual-board-trustee*

# THANKS TO OUR PRESENTING PARTNERS

CHESTER COUNTY community FOUNDATION

CA CC Cultural Alliance of Chester County

GREATER WEST CHESTER CHAMBER OF COMMERCE

Phoenixville Community Health Foundation

United Way

United Way of Chester County

ExtonRegion Chamber of Commerce

Southern Chester County SCCCC CHAMBER OF COMMERCE

Restore CHESTER COUNTY

United Way

United Way of Southern Chester County

# BOARD DUTIES

1. **Ensure Legal & Ethical Integrity**
2. **Build a Competent Board**
3. **Determine Mission & Purpose; Ensure Effective Planning; Monitor & Strengthen Programs & Services**
4. **Protect Assets & Provide Financial Oversight**
5. **Ensure Adequate Financial Resources**
6. **Enhance the Organization’s Public Standing**
7. **Select, Support & Evaluate the Chief Executive**

BoardSource, https://boardsource.org/ Washington DC

# OVERVIEW: This Session's Aims

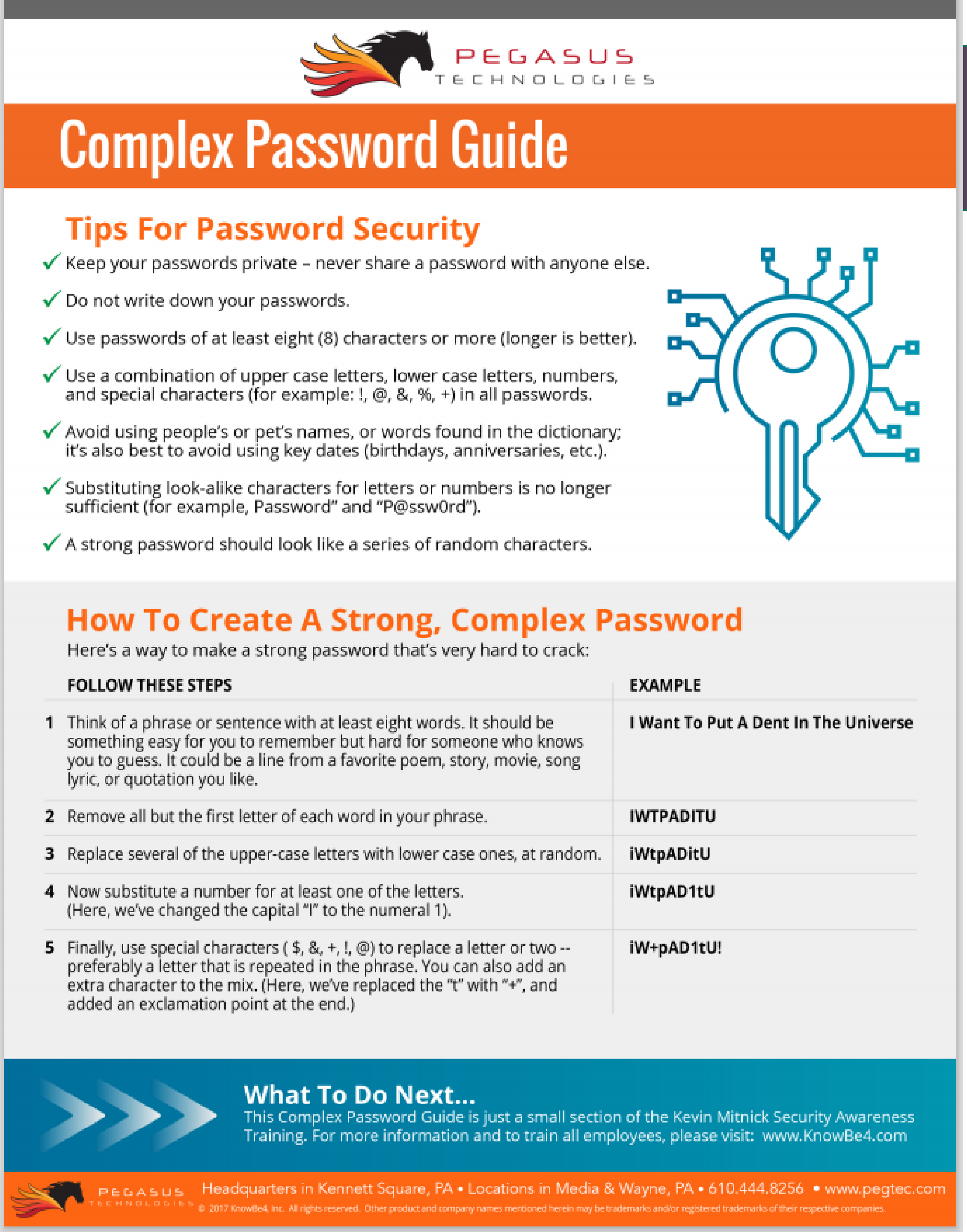
## Cybersecurity in the Context of Governance & Information Technology Issues

Since outside preventative technologies & training are key to preventing ransomware & cyber incidents, raise awareness among Board members for the need to have policies in place and nonprofit staff training in IT areas including:

- complex passwords
- social engineering red flags
- rogue URL red flags
- blocking mobile attacks

Examples:

- how actual attacks hurt local organizations
- why the attacks were successful
- what could have prevented them - technologies & training



PEGASUS TECHNOLOGIES

# Complex Password Guide

## Tips For Password Security

- ✓ Keep your passwords private – never share a password with anyone else.
- ✓ Do not write down your passwords.
- ✓ Use passwords of at least eight (8) characters or more (longer is better).
- ✓ Use a combination of upper case letters, lower case letters, numbers, and special characters (for example: !, @, &, %, +) in all passwords.
- ✓ Avoid using people's or pet's names, or words found in the dictionary; it's also best to avoid using key dates (birthdays, anniversaries, etc.).
- ✓ Substituting look-alike characters for letters or numbers is no longer sufficient (for example, Password" and "P@ssw0rd").
- ✓ A strong password should look like a series of random characters.

## How To Create A Strong, Complex Password

Here's a way to make a strong password that's very hard to crack:

| | FOLLOW THESE STEPS | EXAMPLE |
|---|---|---|
| 1 | Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, movie, song lyric, or quotation you like. | **I Want To Put A Dent In The Universe** |
| 2 | Remove all but the first letter of each word in your phrase. | **IWTPADITU** |
| 3 | Replace several of the upper-case letters with lower case ones, at random. | **iWtpADitU** |
| 4 | Now substitute a number for at least one of the letters. (Here, we've changed the capital "I" to the numeral 1). | **iWtpAD1tU** |
| 5 | Finally, use special characters ( $, &, +, !, @) to replace a letter or two -- preferably a letter that is repeated in the phrase. You can also add an extra character to the mix. (Here, we've replaced the "t" with "+", and added an exclamation point at the end.) | **iW+pAD1tU!** |

## What To Do Next...

This Complex Password Guide is just a small section of the Kevin Mitnick Security Awareness Training. For more information and to train all employees, please visit: www.KnowBe4.com

PEGASUS TECHNOLOGIES Headquarters in Kennett Square, PA • Locations in Media & Wayne, PA • 610.444.8256 • www.pegtec.com

# Social Engineering Red Flags

## FROM

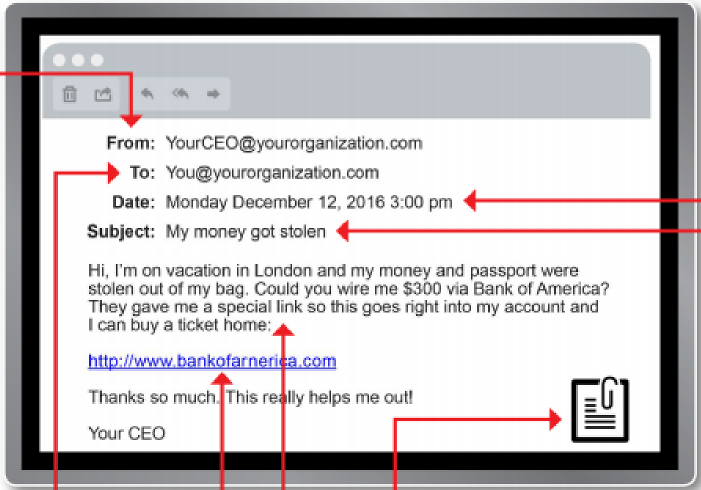
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

## TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



**From:** YourCEO@yourorganization.com
**To:** You@yourorganization.com
**Date:** Monday December 12, 2016 3:00 pm
**Subject:** My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

## ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

PEGASUS TECHNOLOGIES

Headquarters in Kennett Square, PA
Locations in Media & Wayne, PA
610.444.8256 • www.pegtec.com

# THE RED FLAGS OF ROGUE URLs

**Spotting malicious URLs is a bit of an art.** The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

## Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

**Slight Misspellings**

Microsoftnline
<v5pz@onmicrosoft.com>

www.lnkedin.com

**Brand name in URL, but not real brand domain**

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

**Brand name in email address but doesn't match brand domain**

Bank of America
<BankofAmerica@customerloyalty.accounts.com>

**Brand name is in URL but not part of the domain name**

devopsnw.com/login.microsoftonline.com?userid=johnsmith

## URL Domain Name Encoding

https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D

## Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm

## Domain Mismatches

Human Services .gov
<Despina.Orrantia6731610@gmx.com>

https://www.le-blog-qui-assure.com/

## Strange Originating Domains

MAERSK
<info@onlinealxex.com.pl>

## Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndf jnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

## File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.

PDF INV39391.pdf
52 KB

https://d.pr/free/f/jsaeoc
**Click or tap to follow link.**

## Open Redirectors

URLs which have hidden links to completely different web sites at the end.

t-info.mail.**adobe.com**/r/?id=hc347a&p1=**evilwebsite.com**

# 20 Ways to Block Mobile Attacks

**Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!**

## WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

## Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive  privileges to apps unless you truly trust them.

## Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

## Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

## Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

## Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

PEGASUS TECHNOLOGIES

Headquarters in Kennett Square, PA
Locations in Media & Wayne, PA
610.444.8256 • www.pegtec.com

KnowBe4
Human error. Conquered.

# Choosing the Right IT Support Provider

Is the provider the right size for our nonprofit?

Is the provider in it for the long haul?

Does the provider have technical depth?

- balance price against competency

Is the provider diligent with the basics?

- The latest and greatest technology is fun, but there are a lot of "boring" essentials that must be addressed.

Does the provider understand our nonprofit organizational issues?

- Technology is a means to an end, that end being your thriving business.

Does the provider offer service agreements?

- Networks and computers are not a one-shot deal—they always require lots of planning and support.

Does the provider offer Managed Service?

- Today's networks are complicated.
- The provider should offer service and products bundled into one cost.

Can we get direct access to the service provider?

- How exactly does their customer service really work?

Does the provider enjoy what they do?

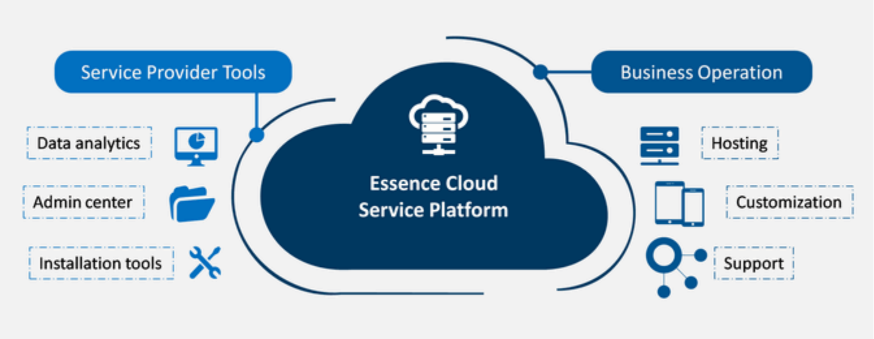
- You need more than competency in a provider.

Does the provider have industry certifications?

- Make sure they are trained and tested professionals.

# Choosing the Right Cloud Service

- Will the provider be in business in five years?
- Can our nonprofit take our data with us when we leave the provider?
- Do we need to pay export fees or cancellation fees to take our data in a usable format?
- What is the protection against price increases or new service charges?
- Is the provider compliant with IT best practices?
- Is all of the data encrypted, including exchanges with partner/integrated websites and services?
- Is the provider compliant with regulatory requirements of our nonprofit organization?
- Is functionality, access, or customization limited because our nonprofit is on a shared platform of a normally customizable product?



- What cyber lessons have we learned amidst the COVID pandemic crisis?
- How does this affect the nonprofit sector as we recover and move forward?

# RESOURCES

## COVID IMPACT & LESSONS LEARNED

https://www.unicef.org/eca/stories/lessons-we-will-learn-pandemic

https://www.aarp.org/health/conditions-treatments/info-2021/lessons-from-covid.html

- Lesson 1: Family Matters
- Lesson 2: Medical Breakthroughs
- Lesson 3: Self-Care Matters
- Lesson 4: Be Financially Prepared
- Lesson 5: Age Is Just a Number
- Lesson 6: Getting Online for Good
- Lesson 7: Working Anywhere
- Lesson 8: Restoring Trust
- Lesson 9: Gathering Carefully
- Lesson 10: Isolation's Health Toll
- Lesson 11: Getting Outside
- Lesson 12: Wealth Disparities' Toll
- Lesson 13: Preparing for the Future
- Lesson 14: Tapping Telemedicine
- Lesson 15: Cities Are Changing

# RESOURCES

## BOARD MATERIALS & SESSIONS

Board of Directors Workshop

Join us virtually to learn best practices for nonprofit board governance!

*Cost is FREE. Space is limited. Register early.*
*chescocf.org/board-workshops*

To register for future Board sessions & obtain prior handouts https://chescocf.org/virtual-board-trustee

Links to useful articles for nonprofit board leaders https://chescocf.org/resources/effective/

| DATE/TIME | TOPIC | SPEAKERS |
|---|---|---|
| | | |
| 11.01.21 | What Donors Look for in | Louise Schorn-Smith, CPA |
| 3:45-5:30 PM | Your Nonprofit Financials | Kathy Wileczek, CPA |
| | | |
| 11.15.21 | Individual Donor | Corrine Sylvia, CFRE |
| 3:45-5:30 PM | Fundraising:  Lean Into | Connie Carter, CFRE |
| | The Trends | Krystine Sipple, CFRE |

**THANKS TO OUR DISCUSSION LEADER & PARTNER**

415 McFarlan Rd., #201, Kennett Square, PA 19348
610.444.8256
info@pegtec.com
https://www.pegasustechnologies.com/

Tech & Cyber Security:
What the Board Needs to Know

Erik Gudmundson,
Pegasus Technologies

# THANKS TO OUR PRESENTING PARTNERS

CCF CHESTER COUNTY community FOUNDATION

CA CC Cultural Alliance of Chester County

GREATER WEST CHESTER CHAMBER OF COMMERCE

Phoenixville Community Health Foundation

United Way

United Way of Chester County

ExtonRegion Chamber of Commerce

Southern Chester County SCCCC CHAMBER OF COMMERCE

Restore CHESTER COUNTY

United Way ™

United Way of Southern Chester County