What's in Your Cybersecurity Toolbox

Michael Bechtel
Information Security Analyst

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

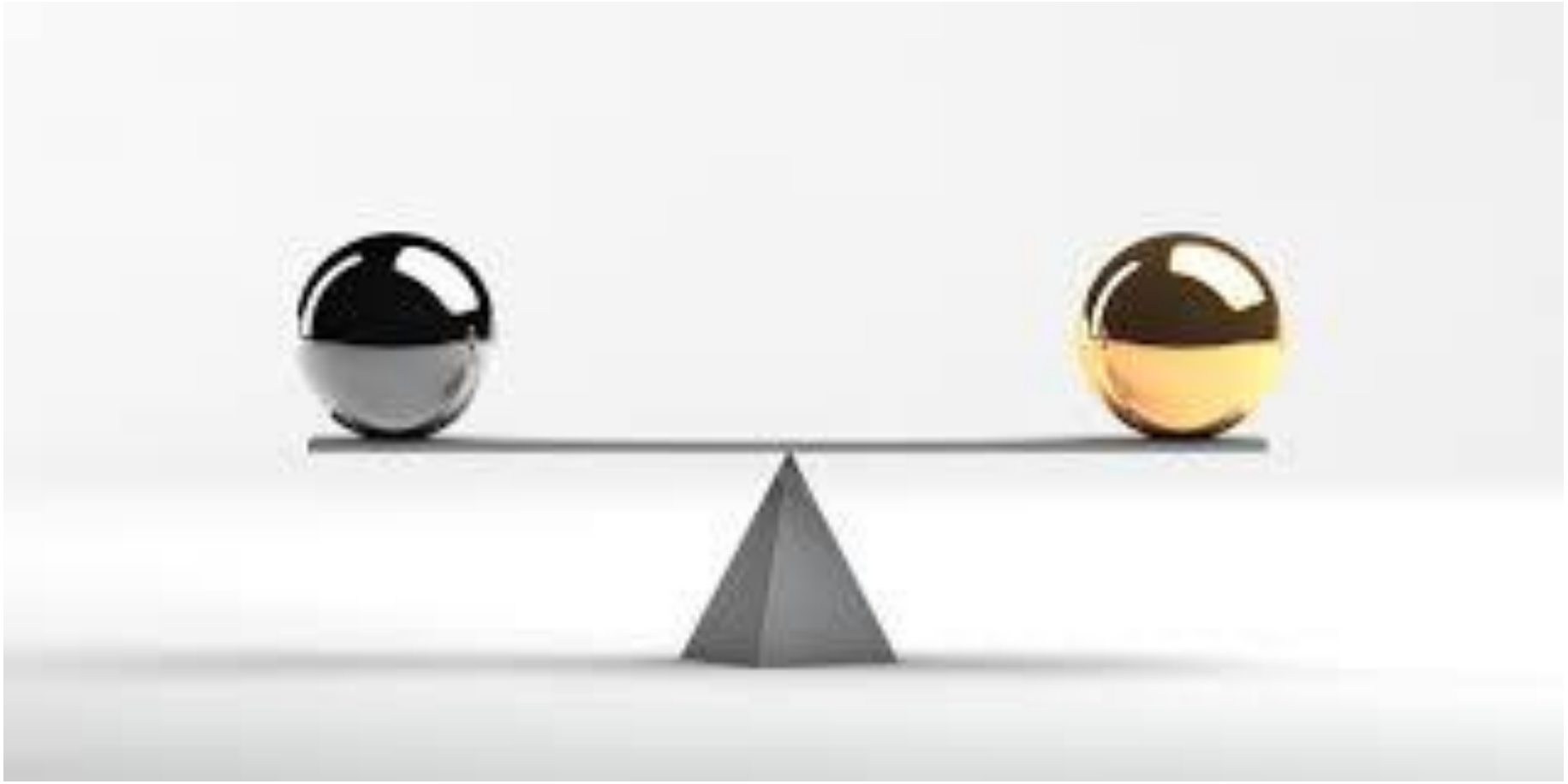
"What's In Your Cybersecurity Toolbox" discussed in this presentation is the current version with effective date of 9/20/2022.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

Agenda

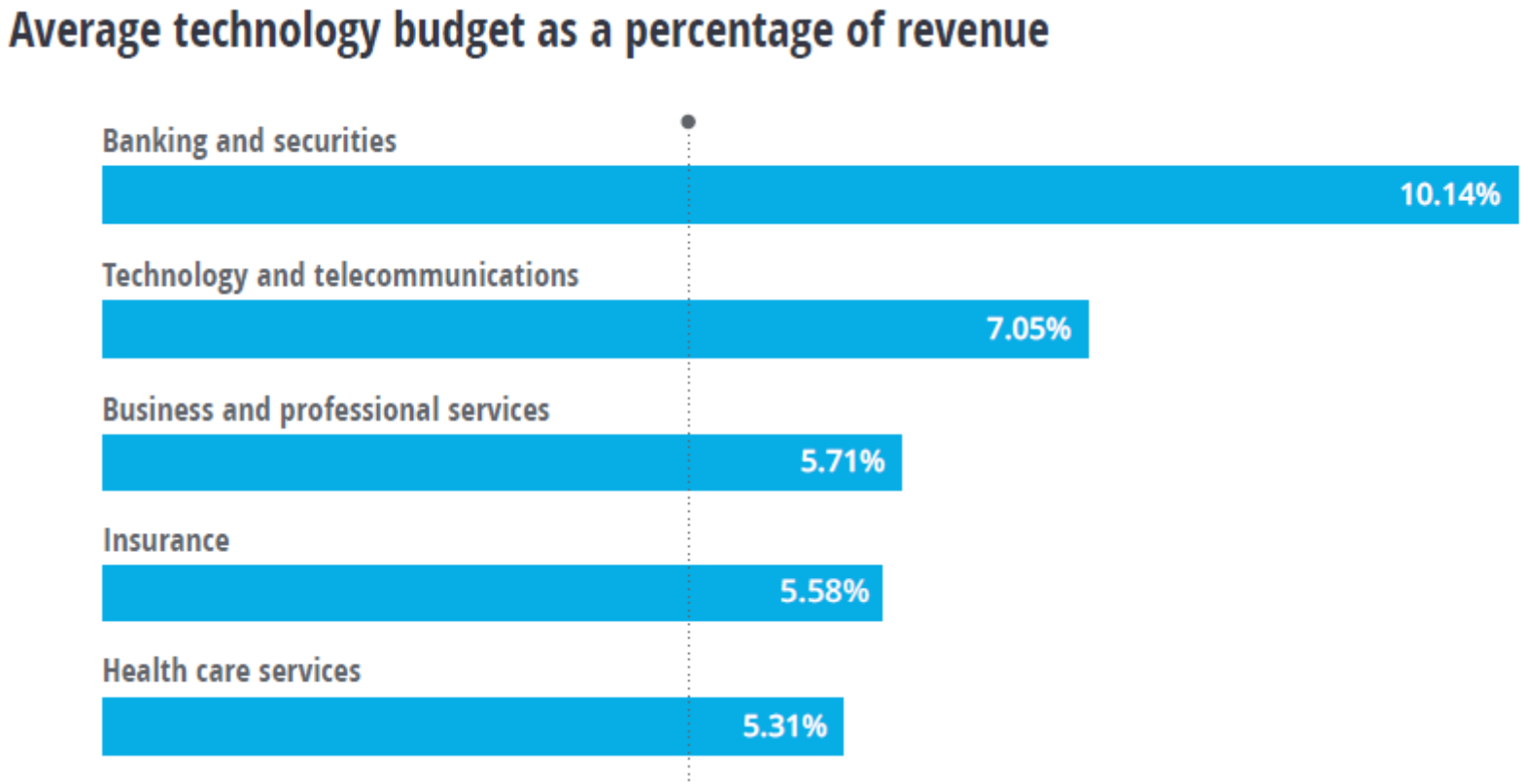
- Budget vs Breach
- What's in Your Toolbox
- Websites and Podcasts
- Security Awareness Training
- Questions

Finding Balance



Budget vs Breach

Budget vs Breach



Budget vs Breach

- Average IT budget is 10% of Company revenue

- Average IS budget is 10% of the Company IT budget

  - $1,000,000 Company income
  - $100,000 IT Budget
  - $10,000 IS Budget

Budget vs Breach

- About 1 IT Employee for every 25 Company Employees

- About 1 Security Employee for every 15 IT Employees

    - 375 Company Staff
    - 25 Information Technology Staff
    - 1 Information Security Staff

Budget vs Breach

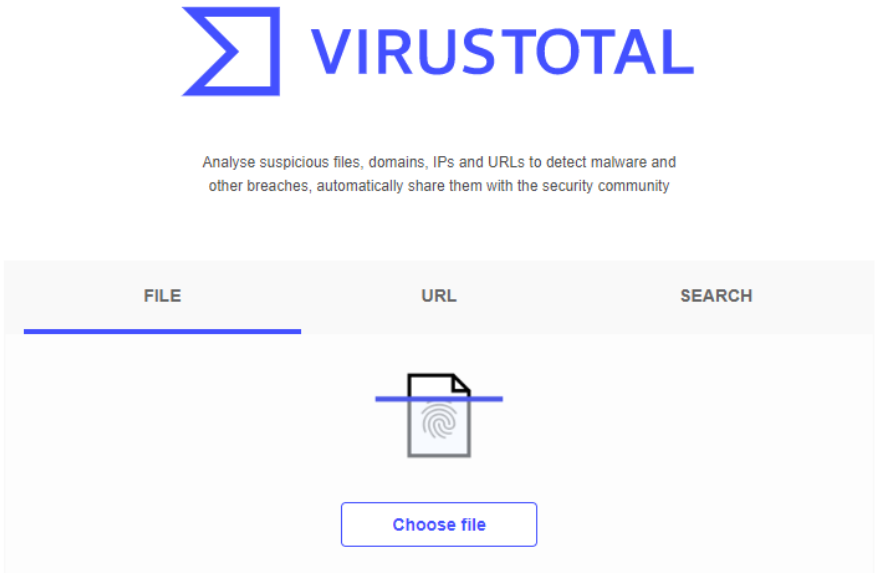
- IBM Security's 17th annual "Cost of Data Breach" report
  - Studied 550 organizations that fell victim between March 2021 & 2022

- $4.35 Million was the average cost
  - 83% of those studied had more than one breach
  - 60% reported an increase in customer prices
  - $2.66 million saved by organizations with well documented and practiced incident response program

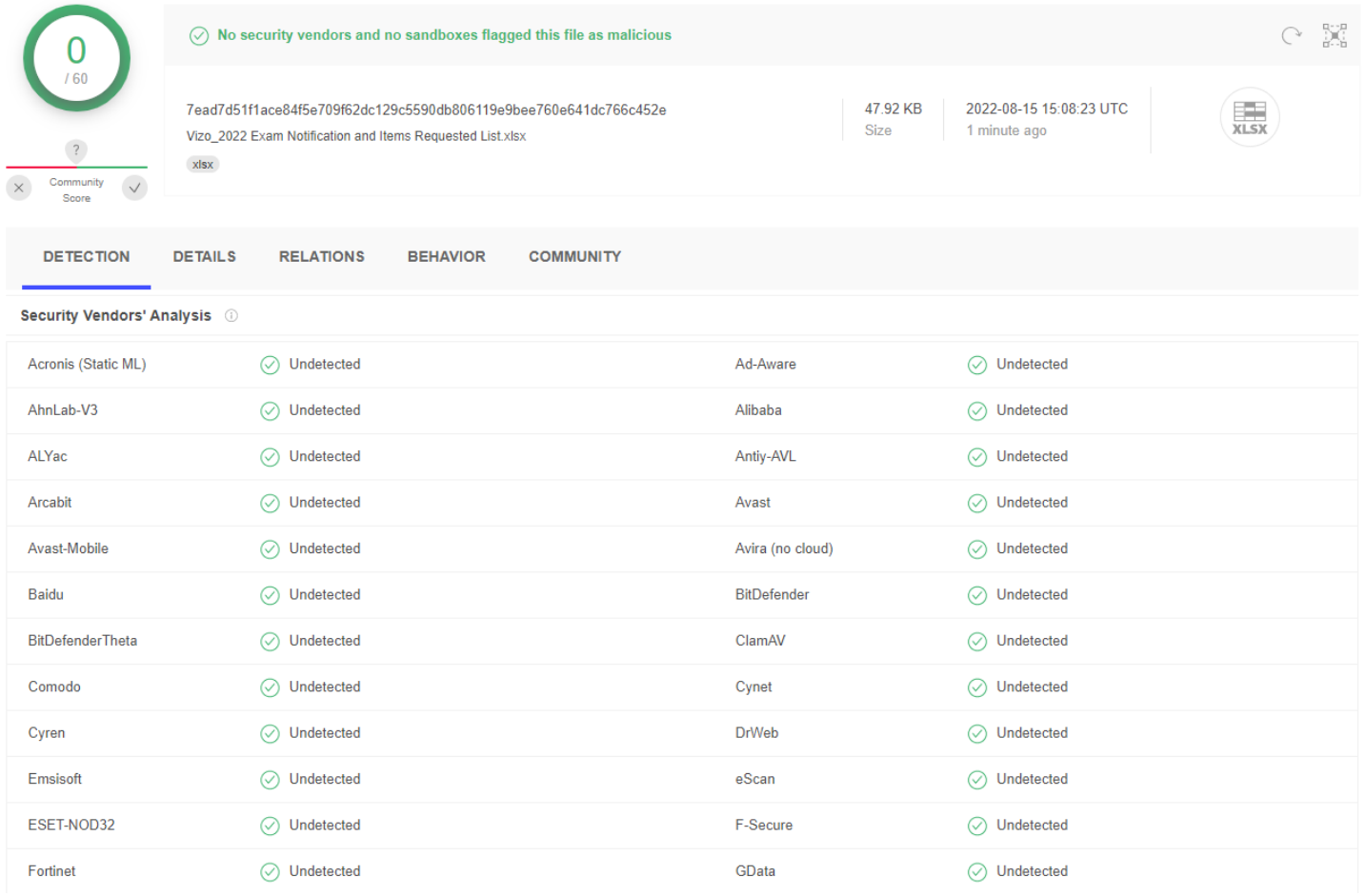
What's In Your Toolbox?

Security Toolbox

- Virus Total
  - Operated by Google
  - Inspects items against 70+ AV engines and domain blockers



Security Toolbox



Security Toolbox

- Malwarebytes
  - Free Trial for active protection
  - Manual scans and removal tool

- Microsoft Defender for Windows
  - Built-in protection
  - Auto updates as part of Windows OS

Security Toolbox

- Cisco Talos Intelligence
  - Spam & Malware Hosts
  - IP & Domain Reputations

- Qualys SSL Labs
  - TLS & SSL Tests
  - Encryption Level

Security Toolbox

- Angry IP Scanner
  - Network IP and Port Scanner
  - Inventory – what's on my network

- KeePass
  - Password Manager
  - Encrypted Storage

Security Toolbox

- Manage Engine MDM+
  - 25 Devices Free Forever
  - Configuration and Management

- MXToolbox
  - DNS – SMTP – URL – IP/Host
  - Troubleshooting Tool

Security Toolbox

- Have I Been Pwned
  - Password
  - Email & Phone Number

- Spiceworks
  - Ticketing System
  - Device Inventory
  - Network Topology Diagrams
  - Device Health and Resource Use

Websites and Podcasts

Websites and Podcasts

“Now I Know……

……”And Knowing is Half the Battle!”

Websites - Federal

Complaint Referral Form
Internet Crime Complaint Center

Homeland Security

- Subscribe to Alerts
- Report Cyber Issues
- Shields UP
- Cybersecurity Action Plans for Small Businesses

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Vizo financial

Websites – National and State

- Local Chapters – Info Sec Conf
- Information Sharing
- State Police Cyber Crime

Websites – News and Information

The Hacker News

BLEEPINGCOMPUTER

threatpost

DARKReading

KrebsonSecurity
In-depth security news and investigation

naked security by SOPHOS

Vizo financial

Podcasts

- Current Events and Education

Podcasts

- Deeper Dives

Security Awareness Training

Security Awareness Training

- NCUA 748 Part A – at least annually

- Foundations of Security Awareness
  - How to Better Identify a Threats
  - Understanding how to React and who to Report to
  - Understand your role in the Information Security Program

- Be Diligent
  - Periodically review the latest security policies and procedures.
  - Current reported threats from CISA / FS-ISAC / NCUA

Security Awareness Training

- **Share the Information you have with others:**
  - Nigerian Prince Email
  - Do you share everyday examples you see?
  - Part of the Bad Actors' success is based on our lack of knowledge

Security Awareness Training

- **Learning to Spot the Difference (more)**
  - Which One is Correct?
  - https://www.paypal.com/
  - https://www.paypal.com/

Security Awareness Training

- **Learning to Spot the Difference (more)**

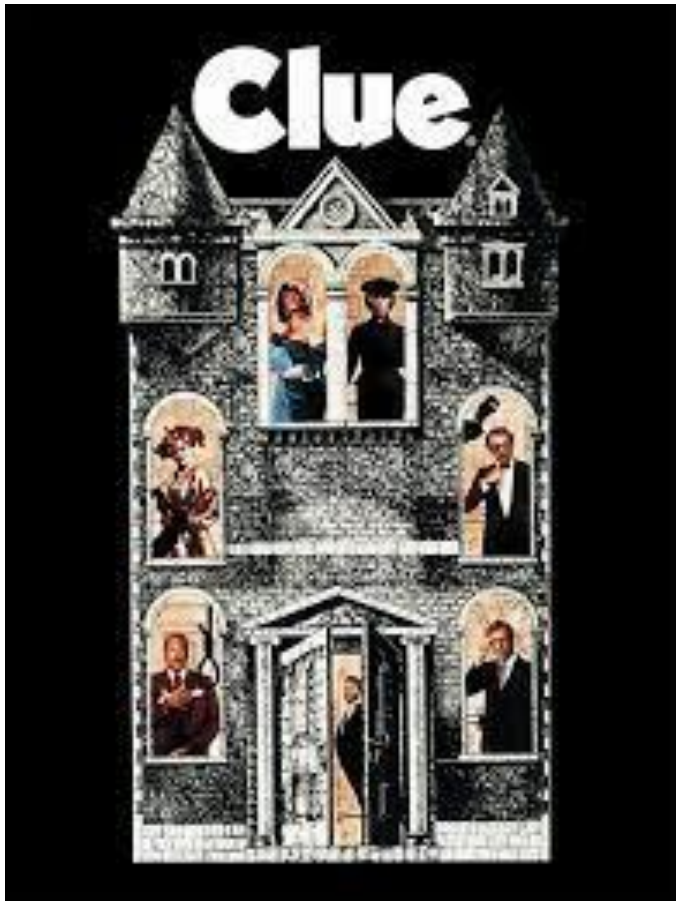
  - Which One is Correct?

  - https://www.paypal.com/ (Correct)

  - https://www.paypal.com/ (Incorrect – capital i, not lower-case L)

Social Engineering

Social Engineering



Social Engineering

- Question to ask and answer before clicking
  - Who:
  - What:
  - When:
  - Where:
  - Why:
  - How:

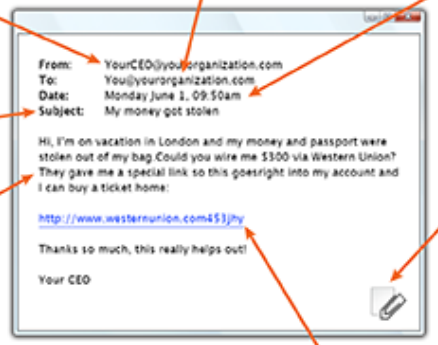
Social Engineering Red Flags

KnowBe4
Human error. Conquered.

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 hadn'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, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

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 these types of attachment(s).)
- 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?

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" & "n".

Passphrases

Schrodinger's Passphrase

- A passphrase is both Good and Bad at the same time.
- The only way to know if a passphrase is good would be to show it to someone else and have it verified.
- This automatically makes it bad because someone else knows the passphrase.

Better Passphrase Habits

- Minimum Length and Maximum Life
  - If 8 is good and 12 is better, does that make 24 best?
    - Longer passphrases do not make better ones
      - 8 character / no complexity = 29.02 seconds to brute force*
      - 10 character / no complexity = 10.45 hours to brute force*
    - Complexity makes shorter passphrases better
      - 8 characters / complexity = 18.62 hours to brute force*
      - 10 characters / complexity = 19.24 years to brute force*
  - Life = Length + Complexity

(*Assuming 100 billion guesses/sec)

Better Passphrase Habits

- 2FA vs MFA – Choose wisely
  - Something you ARE / KNOW / HAVE
  - 2FA superior to MFA
  - Weaker
    - Security Questions
    - Email
  - Stronger
    - Physical Token
    - Software Token

Questions

Recording Available

Contact Information

- Michael Bechtel
- Information Security Analyst
- mbechtel@vfccu.org
- Toll-Free (800) 622-7494 ext. 1101
- Website: www.vfccu.org/solutions_mobile/risk_management.html