THE FLORIDA BAR

CYBERSECURITY FOR SMALLER LAW FIRMS

Practical advice for protecting your law firm
(and your own finances) from online threats

Special Edition for Increased Vigilance due to recent and upcoming events such as the war in Ukraine and the mid-term elections

Daniel Cohn, Solutions Architect
Dynamic Quest

DYNAMIC
QUEST™

AGENDA

- **Cybersecurity: The Partners, The IT Department, and You**
- **Why Law Firms Are Targets**
- **Defense In Depth – The Layers of Cybersecurity Protection**
- **A Brief Overview of Cybersecurity Technologies**
  - ***What IT is doing behind the scenes***
- **What YOU Should Expect and Practical Advice on What To Do**
  - ***On the web, in your email, on your phone, and in person***
  - ***Why current events matter***
  - ***Key things to remember***
- **Q & A**

CYBERSECURITY PERCEPTIONS

- **Most people outside of the IT department know cybersecurity is a big deal but…**
  - Overhype it or minimize it
  - Have unrealistic expectations of what's possible

- **Most people outside of the IT department view IT as a "black box"**
  - Don't know how IT works
  - Consider IT a budget drain (or worse)
  - Assume it is kind of like magic

But…

> "Any sufficiently advanced technology is indistinguishable from magic."

Arthur C. Clarke
Clarke's Third Law
Profiles of the Future
(revised edition, 1973)

THE PARTNERS, THE IT DEPARTMENT, AND YOU

- The Partners set the overall culture
  - Viewing IT as foundational for success
  - Fostering a “culture of security”
  - Serving as an example of learning about IT and Cybersecurity on multiple levels
- The IT Department advises the Partners and carries out the mission
  - Balancing business needs, productivity, and security
  - Evaluating and implementing technology
  - Monitoring for, reacting to, and reporting on compliance and effectiveness
- You
  - Being a part of the “culture of security”
  - Staying up to date via training
  - Understanding how important YOU ARE

THE STAKEHOLDERS

Partners and Owners

- Want to be sure investments are secure
- Need to see due diligence and awareness

Government and Oversight

- Need proof of compliance
- Can demand audits and testing
- Can exact penalties

Management

- Protection of assets and reputation
- Competitive edge

Staff

- Need data to be secure, reliable, and available
- Need to get things done without onerous security protocols
- Need technology to increase productivity and service

Clients

- Expect information to be secure
- Will take business elsewhere if concerned

WHY LAW FIRMS ARE TARGETS

LAW FIRMS are prime cybersecurity targets

- Deal with large sums of money
- Often do large electronic transfers
- Have a client base that may also be lucrative targets

SMALLER firms are prime cybersecurity targets

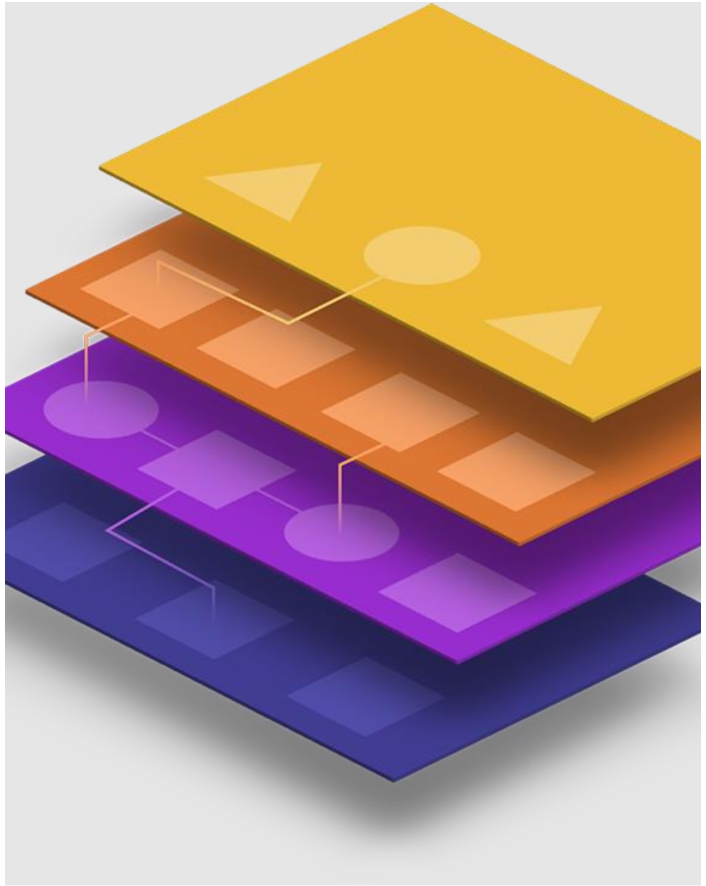
- Tend to have less awareness, monitoring, and protection
- Often can’t afford or choose not to make the necessary investments

DEFENSE IN DEPTH

Top Layers

- Physical
- Managerial
- Technological
- The Human Element

All are interrelated…



DEFENSE IN DEPTH

Physical

- Standard physical security for your office
- Make it hard for someone to steal equipment or information
  - Don’t leave phones and laptops unattended in open areas
  - Cable locks
  - Locked doors / Badge access
  - Alarm systems and cameras
  - Clean desk policy
  - No Post-it® notes

DEFENSE IN DEPTH

Physical

- Physical cybersecurity protection of your assets
  - Restricting access to devices
    - Especially outside of your buildings
    - And don’t forget USB ports
  - Restricting access to the network
  - Screen locking and privacy filters
- Biometrics vs PINs
  - Legal ramifications
- Related management policies and technological safeguards

DEFENSE IN DEPTH

Managerial

- Cybersecurity as a key element of all projects
- Partner commitment to a culture of security
- Documented policies and procedures
  - Especially employee agreements and technology usage agreements
- The “business” of IT and Cybersecurity
  - Budgets, monitoring and metrics, analysis, review
- Cybersecurity incident response plan

DEFENSE IN DEPTH

Technological

- Know what systems to protect
- Understand the differing Cybersecurity technologies
- Finding the “right” Cybersecurity products
- Finding the “right” Cybersecurity expertise
- Deployment / Management / Monitoring
- Testing
- Cybersecurity incident response plan
- Disaster recovery plan

DEFENSE IN DEPTH

The Human Element

- Your people are THE KEY to your law firm's cybersecurity success

- Foster a "culture of security"
- Provide tools and continuous training
- Make security easy
- Make security reporting easy
- Give your people a sense of ownership
- Incentivize security

A BRIEF OVERVIEW OF CYBERSECURITY TECHNOLOGIES

What Systems Do You Need To Protect?

- Vendor cloud systems – especially email
- Hosted virtual and physical servers
- Physical on-premise networks
- Wireless on-premise networks
- On-premise servers
- On-premise storage devices
- On-premise workstations, laptops, and corporate mobile devices
- Personal workstations, laptops, and mobile devices (known as “Bring Your Own Device”)

- Remote connections
- Local connections
- Backup systems and data
- Domain information
- Data wherever it may reside
- Identities and Passwords
- Internal systems knowledge
- Internal expertise
- Your people

A BRIEF OVERVIEW OF CYBERSECURITY TECHNOLOGIES

A Sampling of Cybersecurity Technologies

- Antivirus / Antimalware
- Antispam
- Firewall
- Virtual Private Network (VPN)
- Multi Factor Authentication (MFA)
- Password management systems
- Dark Web monitoring
- DNS filtering
- Network Access Control
- Security Awareness Training (SAT)
- Continuous operating system and 3rd party software maintenance and patching
- Secure image-based local and cloud backups
- Monitoring and alerting systems
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC)
- Asset and document management systems
- Digital Rights Management (DRM)

A BRIEF OVERVIEW OF CYBERSECURITY TECHNOLOGIES

The Takeaway

There are a lot of systems and "things" to protect

Not all of them are obvious

Any of them can be a conduit for a cybersecurity breach

Which Means…

There are a lot of technologies that will make you more secure

In a perfect world, you'd have them all

But you should always have "**The Basics**" and then add more where you can

A BRIEF OVERVIEW OF CYBERSECURITY TECHNOLOGIES

The Basics

- **Antimalware and Firewall**
  - Watching for and stopping bad things coming in
- **Antispam and MFA**
  - Reducing the clutter and stopping the #1 way hackers get in
  - Making sure it’s really you
- **DNS filtering**
  - Making sure you only go to safe places and blocking ransomware
- **Dark Web monitoring**
  - Your canary in the coal mine
- **Continuous maintenance and patch**
  - Fixing the holes in systems that hackers exploit
- **Monitoring and alerting**
  - 24/7/365 “eye in the sky,” watching out for suspicious activity

A BRIEF OVERVIEW OF CYBERSECURITY TECHNOLOGIES

The Basics

- **Secure local and cloud backup**
  - The ultimate defense: “Like it never even happened”
- **Security Awareness Training**
  - The right tools, training, and knowledge to make everyone a security defender

SO WHAT SHOULD YOU LOOK OUT FOR?

- Pay attention to more than just your PC…
  - Any “smart device”
  - The usual suspects
    - Emails and web sites
  - But also…
    - Web apps
    - Cellphone
    - Telephone
  - As well as…
    - People!

AND WHERE SHOULD YOU BE LOOKING OUT?

- And not just at work…
  …because we're on 24/7

  - Working from home
  - Working on the road
  - Catching up while waiting in line
  - Checking in while at the gym, or a restaurant, or at a friend's place

  - You get the idea…

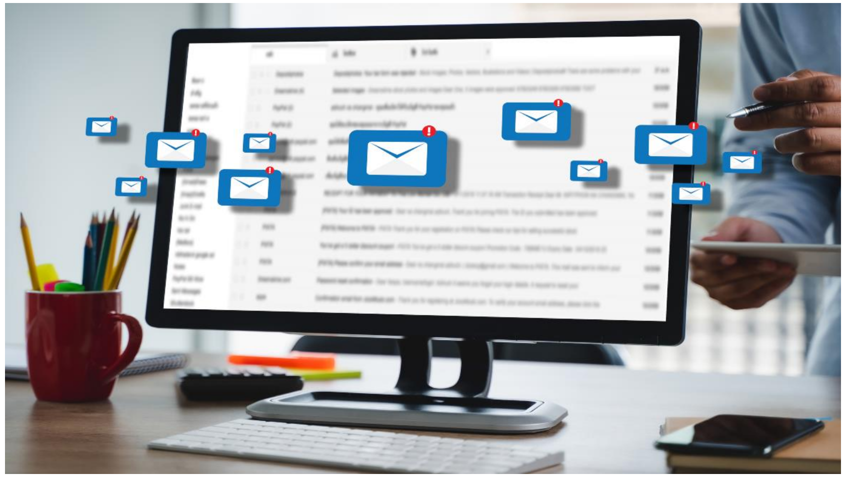
SMART DEVICES

- PC’s and laptops and tablets
  - Windows, Apple, Android, etc
- Smartphones
  - iPhone, Android, Pixel, etc
- Wearables
- Gaming systems
- Streaming TV’s and devices
- Wireless “gadgets” and appliances
- USB sticks and devices

THE USUAL SUSPECTS

- Email
- Websites
- Social Media
- Web apps (especially ad-supported)

- **The Danger**
- Familiarity = Complacency
- Rote memory = Clicking “automatically”
- Designed to connect and take action = Links, attachments, and downloads



PRACTICAL ADVICE: BUSINESS VS PERSONAL

- Keep your business and personal worlds **separate**
  - Don’t use the firm’s email for personal services
  - Don’t use unmanaged personal devices for business purposes
  - Don’t use the firm’s devices for personal tasks

PRACTICAL ADVICE: TIME OUT!

- Stop, Breathe, and Think
  - “Fear = Fake”
  - “If it has a link, stop and think”
  - It doesn’t matter who it is from:

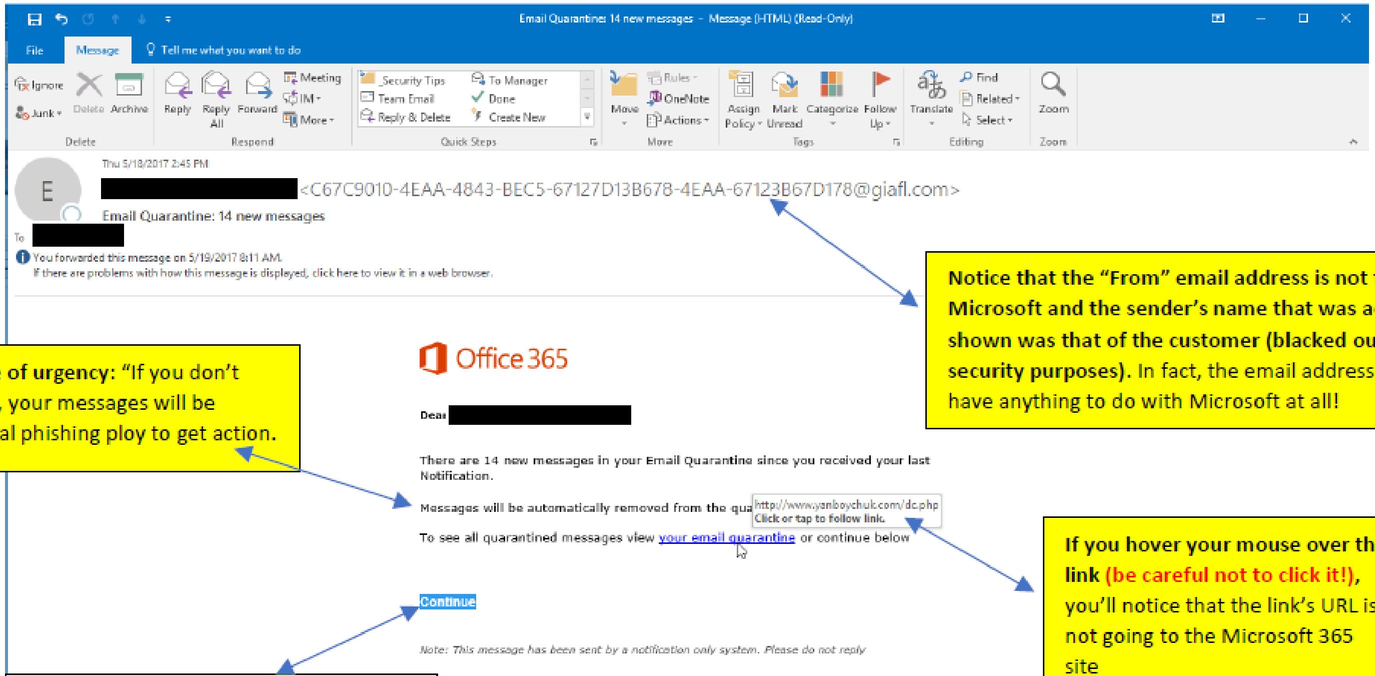
    If it involves money, passwords, or identity, verify it first **without** using “Reply”

PRACTICAL ADVICE: SLAM!

- **SLAM** the scam!

- **S**ender
- **L**inks
- **A**ttachments
- **M**essage

- Hover over **S**ender and **L**inks to reveal what they really are



Thu 5/18/2017 2:45 PM

[redacted] <C67C9010-4EAA-4843-BEC5-67127D13B678-4EAA-67123B67D178@giafl.com>

Email Quarantine: 14 new messages

To [redacted]

You forwarded this message on 5/19/2017 8:11 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.

Office 365

Dear [redacted]

There are 14 new messages in your Email Quarantine since you received your last Notification.

Messages will be automatically removed from the qua

http://www.yanboychuk.com/dc.php
Click or tap to follow link.

To see all quarantined messages view your email quarantine or continue below

Continue

Note: This message has been sent by a notification only system. Please do not reply

Notice the sense of urgency: "If you don't take action soon, your messages will be deleted". A typical phishing ploy to get action.

Notice that the "From" email address is not from Microsoft and the sender's name that was actually shown was that of the customer (blacked out for security purposes). In fact, the email address doesn't have anything to do with Microsoft at all!

If you hover your mouse over the link (be careful not to click it!), you'll notice that the link's URL is not going to the Microsoft 365 site

The URL connected to this button goes to the same bogus site as the link. Again, hovering your mouse over the button will reveal the link

CELLPHONE AND TELEPHONE

- Phishing = Attack via email
- Vishing = Attack via telephone call
- Smishing = Attack via SMS text
- All designed to steal information

- **The Danger**
- Better Quality = Harder to spot
- Lots of Public Info = Very convincing
- We're Busy = Less likely to stop and verify who's sending, calling, and texting

PRACTICAL ADVICE: TIME OUT!

- **Emails AND Calls AND Texts**

- Stop, Breathe, and Think

  - “Fear = Fake”
  - “If it has a link, stop and think”

  - It doesn’t matter who it is from:

    If it involves money, passwords, or identity, verify it first **without using “Reply”** or by **calling a known good number**

PRACTICAL ADVICE: NOT OFFICIAL BUSINESS!

- The IRS, Sheriff, Police, and Postal Service do not send emails or texts
  - They also don’t call with threats
- Microsoft and Internet companies are not monitoring your PC for threats
  - They also don’t call to help you fix them
- The partners will not email you asking you to do an emergency wire transfer
  - They also don’t ask for you to purchase and send gift cards on their behalf

PEOPLE

- Criminals who masquerade as:
  - Clients, vendors, management
  - Delivery people (especially food)
  - Authority figures (police, etc)

- **The Danger**
  - We like to be helpful, we tend to be trustful, and we don't want to get in trouble
  - Criminals are good at crafting scenarios to capitalize on that

PRACTICAL ADVICE: KNOW WHO YOU'RE DEALING WITH

- **Identify, Verify, and Escort**
- Check in / Check out
- Verify ID and that the person should be there
- Assign escorts for untrusted visitors
- When in doubt, double-check

- **Don't make it easy**
- Screen lock, clean desk, "pinned" items
- Watch for illicit camera use

SPECIAL FOCUS: DISCLAIMER

The following information is provided to help businesses and other organizations maintain security.

No judgment or opinion is expressed or implied by the inclusion or exclusion of any named entities.

Dynamic Quest apologizes in advance if any content is considered offensive or insensitive by viewers of this webinar.

SPECIAL FOCUS: THE INVASION OF UKRAINE BY RUSSIA

- **Extra Vigilance**
- Increased cyberattacks in general
- Russian “revenge” for sanctions
- Russian cybermilitary strikes
- “Piling on” by other nations and enemies
  - North Korea, Iran, China, etc
  - ISIS, Taliban, etc
  - Domestic extremists
  - Anonymous, Darkside, Revil, etc

An attack from all sides
BELARUS
RUSSIA
UKRAINE
Kyiv
MOLDOVA
ROMANIA
Site of shelling
Russian troops
Tanks
Russian military positions
Mariupol
Crimea
Annexed by Russia in 2014
Area held by Russian-backed separatists

SPECIAL FOCUS: THE INVASION OF UKRAINE BY RUSSIA

- **Extra Vigilance**
- High stress
- Fast breaking news
- Passionate opinions
- Natural human curiosity
- Multiple sources of information
  - News
  - Government
  - Social Media

An attack from all sides
BELARUS
RUSSIA
UKRAINE
Kyiv
MOLDOVA
ROMANIA
Site of shelling
Russian troops
Tanks
Russian military positions
Crimea
Annexed by Russia in 2014

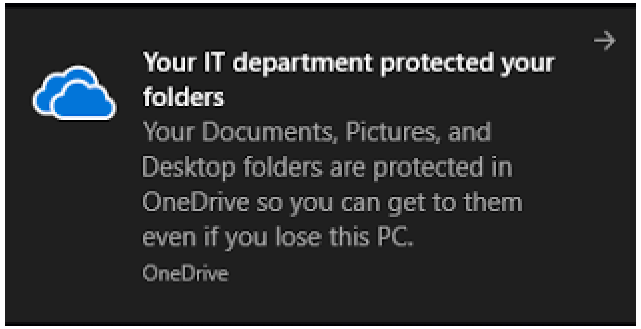
SPECIAL FOCUS: THE INVASION OF UKRAINE BY RUSSIA

NEW TONIGHT
BEWARE ONLINE FUNDRAISER SCAMS
ALABAMA ORGANIZATION SCAMMED TRYING TO DONATE TO UKRAINE
waaytv.com

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left
02:23:59:06

DEPARTMENT OF JUSTICE
FIDELITY BRAVERY INTEGRITY
FEDERAL BUREAU OF INVESTIGATION

U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE


Your IT department protected your folders

Your Documents, Pictures, and Desktop folders are protected in OneDrive so you can get to them even if you lose this PC.

OneDrive

SPECIAL FOCUS: THE INVASION OF UKRAINE BY RUSSIA

What To Watch Out For: Anything With A Link!

- Breaking news alerts
- Urgent charitable appeals
- Warnings from government agencies
- Warnings from your IT department
- A “hot post” on social media
- Warnings on your PC or cellphone
- Unexpected Multi Factor Authentication (MFA) prompts
- Texts confirming donations or shipments
- Texts to make donations

SPECIAL FOCUS: THE INVASION OF UKRAINE BY RUSSIA

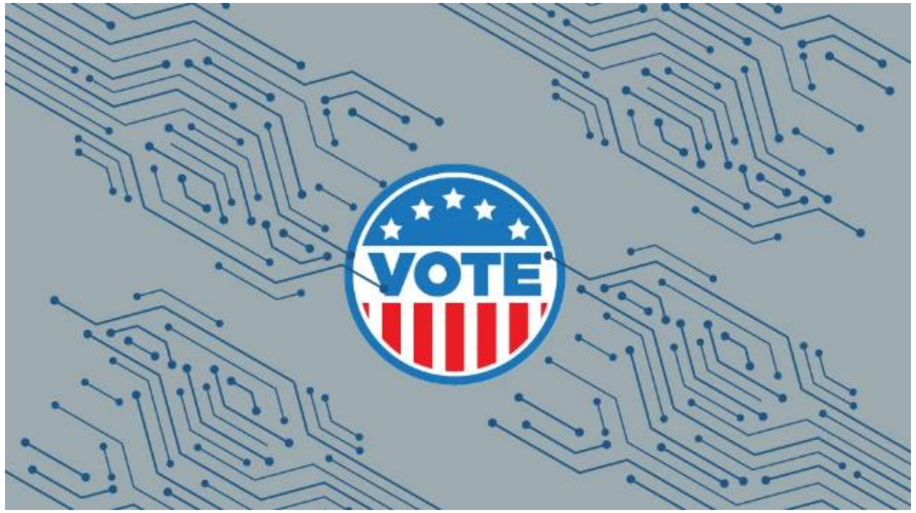
- **Be vigilant but not paranoid**

- Trust and verify

- **Go to official news sites**
- **Go to official government websites**
- **Verify charities online and stay with known entities**
- **Check with your IT department**
- **Call people who reach out online**

SPECIAL FOCUS: THE MID-TERM ELECTIONS

- **Extra Vigilance**
- Increased cyberattacks in general
- Questions and misinformation about election security
- “Piling on” by nations and enemies
    - Russia, North Korea, Iran, China, etc
    - ISIS, Taliban, etc
    - Domestic extremists
    - Anonymous, Darkside, Revil, etc



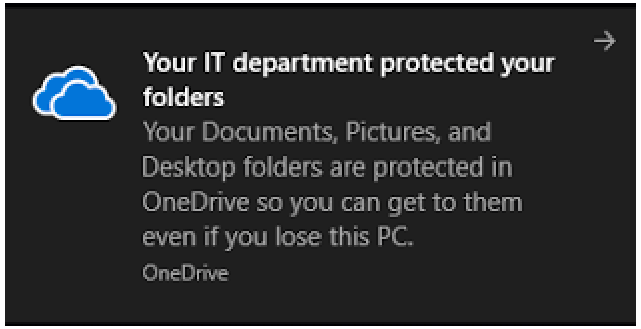
SPECIAL FOCUS: THE MID-TERM ELECTIONS

- **Extra Vigilance**
- Fast breaking news
- “Hot button” issues / Passionate opinions
- Natural human curiosity
- Multiple sources of information
  - News
  - Political Organizations
  - Campaign Feeds
  - Social Media

SPECIAL FOCUS: THE MID-TERM ELECTIONS

FRAUDSTERS USE ELECTION SEASON TO TARGET UNSUSPECTING PEOPLE WITH POLITICAL SCAMS
VOTE
VOTE
VOTE
VOTE
VOTE
VOTE

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left
02:23:59:06



Your IT department protected your folders

Your Documents, Pictures, and Desktop folders are protected in OneDrive so you can get to them even if you lose this PC.

OneDrive

SPECIAL FOCUS: THE MID-TERM ELECTIONS

What To Watch Out For: Anything With A Link!

- Breaking news alerts
- Political donation appeals
- Warnings from government agencies
- Warnings from your IT department
- A “hot post” on social media
- Warnings on your PC or cellphone
- Unexpected Multi Factor Authentication (MFA) prompts
- Texts confirming donations or shipments
- Texts to make donations

SPECIAL FOCUS: THE MID-TERM ELECTIONS

- **Be vigilant but not paranoid**

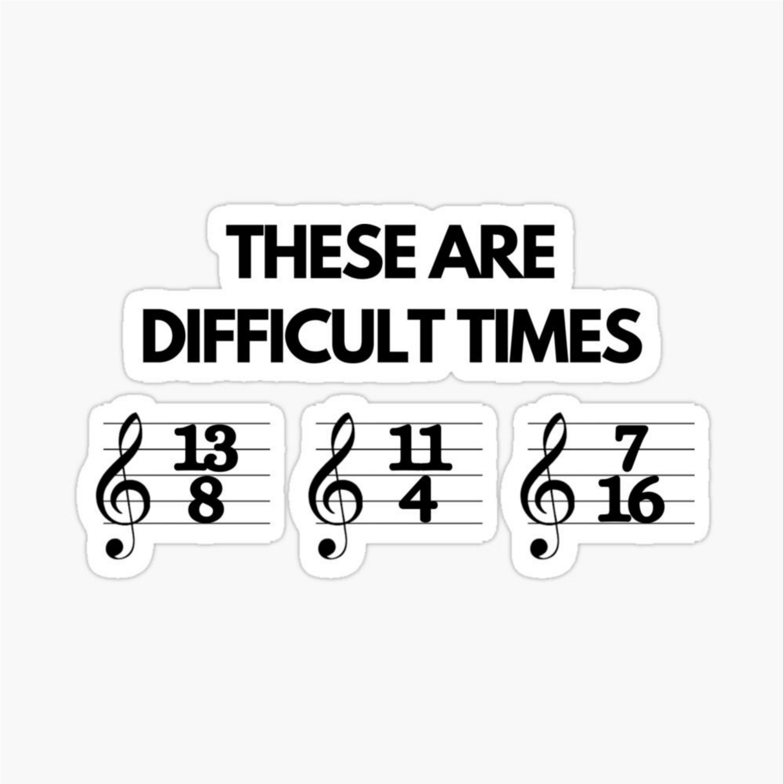
- Trust and verify

- **Go to official news sites**
- **Go to official government websites**
- **Verify political organizations online and stay with known entities**
- **Check with your IT department**
- **Call people who reach out online**

SPECIAL FOCUS: OTHER CURRENT EVENTS

- **Extra Vigilance**

- Potential economic recession
- Recent Supreme Court decisions
- COVID 19 and variants
- Climate change
- Recent natural disasters



PRACTICAL ADVICE: TIME OUT!

- **Emails AND Calls AND Texts**

- Stop, Breathe, and Think

  - “Fear = Fake”
  - **“Outrage might be Fake”**
  - “If it has a link, stop and think”

  - It doesn’t matter who it is from:

    If it involves money, passwords, or identity, verify it first **without using “Reply”** or by **calling a known good number**

MORE PRACTICAL ADVICE

- Passwords
  - Don’t reuse passwords or make minor changes
  - Make them long but easy to remember
    - Song lyrics
    - Unusual substitutions
  - Don’t write them down or keep them in spreadsheets
    - Password managers are awesome!

CREATE THE CULTURE OF SECURITY

- **Conduct security tests all the time**
  - **Create the expectation that emails, texts, etc are fake**
  - Keep your staff on their toes
  - Test for phishing, vishing, smishing, and USB use
- **Reward the people who pass**
- **Educate (and don't punish) the people who don't**
- **Reward people who double-check**

QUESTIONS AND ANSWERS

FOR MORE INFORMATION…

Please reach out to The Florida Bar at

legalfuel@floridabar.org