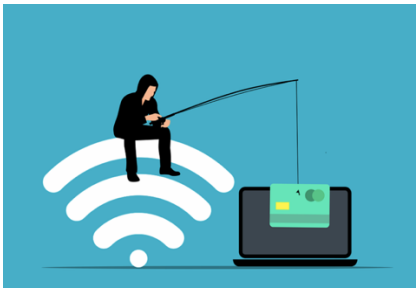
Phishing, Pharming, Smishing, and Other Cyberattacks that can Ruin a Lawyer's Career

Honorable Judge Mary Evans, Esq.
Mira White, Esq. B.C.S., CPA
Michael Shemkus, Esq.
Jeffrey Rapkin, Esq.



OUTLINE

I. FOCUS OF PRESENTATION: <u>As Lawyers, We Have an Enduring Ethical Obligation to Protect Our Client's Private Information.</u>

Getting hacked could mean the end of a lawyer's career. We are being listened to. We are being tracked. We are being hacked. Protect yourself. Protect your clients.

I. Recent implementation of new and unusual scamming techniques: Recognizing how they work is the first step in protecting your clients and your firm.

* Phishing Scams
* Pharming Scams
* Smishing Scams
* Social Media Messenger Scams
* Romance/Online Dating Scam
* Emergency Scams aka "Grandparent Scams"
* Online "Marketplace" Purchase Scams
* "Free" Gift Offers
* Malware Scams
* Advance Fee Scams
* Foreign Money Exchange Scam aka "Nigerian Fraud"
* "Spoofing"
* Scams that target lawyers

II. What is "Social Engineering?" This technique increases the effectiveness of the cybercriminals' hacking techniques.

III. Proliferation of internet-accessed devices, has led to the "Internet of Things," (IOT)

A. What is it? How does it work?
B. Why are these devices connected to the internet? (Who needs a "smart-toothbrush?")
C. Devices are being hacked. The companies' focus is on gathering information to advertise and make money, not on security.

The problem with Alexa, Siri, and your Smart-Toaster: Lawyers are NOT regular people. We took an oath to keep clients' confidences, to protect their secrets, to protect their interests, their sensitive information, their money. It is dangerous to surround ourselves with easy-to-hack internet devices that can listen to us.

IV. Tips, tools techniques for survival in the "malware" age.

* Backup. (You must!) And maintain them!
* Updates
* Trust Account Considerations
* Passwords
* Don't be a Victim of "Social Engineering"
* Other tips, tools, techniques

I. Recently there has been an outbreak of new and creative internet-scamming techniques.

"Smishing?" "Pharming?" These words sound may sound silly, but they represent a growing trend in online crime. Using reputable sources, you will learn what is happening, what is true and what is myth, and most importantly, the tools and techniques you can utilize to *protect yourself* and your firm.

Generally, lawyers have been fairly lucky, so far. Walk into any small-town law firm, you might even find computers running Windows XP and WordPerfect 6. (Shut up, I still use WordPerfect.)

Cybercriminals, for the most part, haven't noticed attorney's trust accounts and the often extremely large sums that are contained within. That will change eventually. It's only a matter of time before the Nigerian Prince sets his sights on the legal community. As lawyers with a genetically-encoded obligation to protect our clients, we owe it to them (and to ourselves) to take all measures possible to protect all of us.

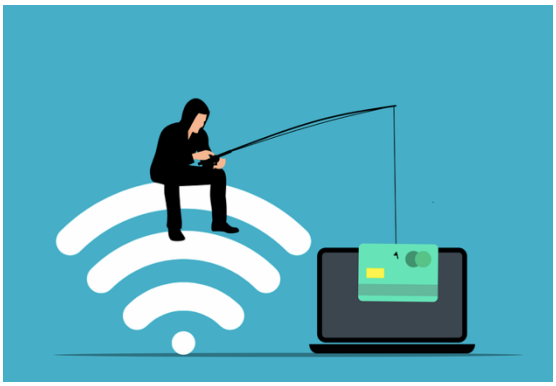
MYTH DISPELLED: Most people think that there are hackers out in the world, using advanced software, coding, and programming to "brute force" attack an unsuspecting victim, that the only thing someone has to do to fall prey is to have a computer, have it turned on, and, of course, have it connected to the internet. This is not the case. The overwhelming majority of hacking is not a criminal someplace using some kind of advanced computers and coding to infiltrate your Dell Inspiron, your HP, or that MacBook Air that is still running OS X El Capitan. (For the love of God, please update)

When a person's computer gets "hacked," it's not the computer that's getting hacked, rather, it is the operator who has been tricked into "opening" the doors to his or her personal data to a malware, ransomware, or some other kind of attack.

In other words, if YOU get hacked, it is because YOU allowed yourself to get hacked. Really, all it takes is a "click" of the mouse, or a "tap" on your screen and cybercriminals are in and digging around your hard drive, looking through your bank account numbers and the pictures of last year's Christmas party.

Recognizing the scam (what it is and how it works) is the first step in making sure you are not victimized.

BE AWARE!



* **Phishing Scams**
* **Pharming Scams**
* **Smishing Scams**
* **Social Media Messenger Scams**
* **Romance/Online Dating Scam**
* **Emergency Scams aka "Grandparent Scams"**
* **Online "Marketplace" Purchase Scams**
* **"Free" Gift Offers**
* **Malware Scams**
* **Advance Fee Scams**
* **Foreign Money Exchange Scam aka "Nigerian Fraud"**
* **"Spoofing"**
* **Scams that target lawyers**

DESCRIPTIONS (For expediency, these are brief, abbreviated descriptions.)

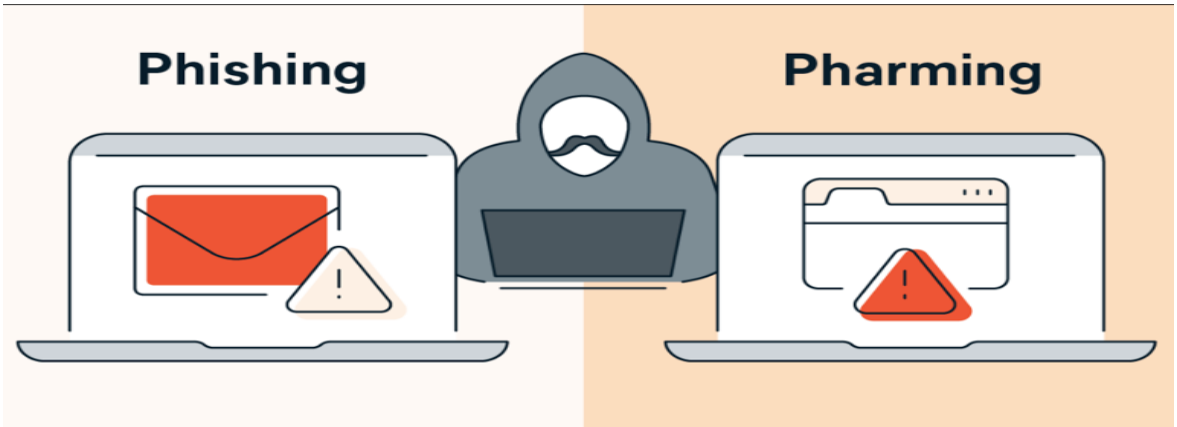
PHISHING:
With a Phishing scam, the criminal poses as a trusted, legal, legitimate, source in order to fool you into providing sensitive data such as your sensitive biographical information, usernames, passwords, banking details or other valuable information. The criminal then uses the information to steal from you (obviously) or commit identity theft. Once a cybercriminal has access to your computer, this kind of attack can also subject you to a malware or ransomware attack, or even an infiltration of your entire network.

PHARMING:
With a "Pharming" attack, malware or some kind of malicious code is installed on a person's computer or server, which then misdirects users to fraudulent websites with the intent of the unsuspecting user inputting personal information. Once on the fake website, important financial information is obtained by the user themselves, who attempt to utilize the site, mistakenly believing that they are on a legitimate website. Phishing and Pharming are similar, but have some key differences in how they work.

Pharming attacks use DNS (domain name system) to redirect users from the intended domain to another (falsely created) website. This is done by using malicious code to add entries which redirect traffic, or which changes the IP address of the intended website to redirect you to the illegitimate website. Pharming works by exploiting the way browsers convert a URL into an IP address via a DNS server. (DNS servers convert the URL or domain name into an IP address, leaving behind a cache so you don't need to go through the server every time you visit the site.) Pharming attacks interrupt this process by redirecting you to spoofed IP addresses that lead to fake websites.

A common Pharming technique is for code sent in a malicious email, which, when "clicked on," modifies the local (host) files on your computer. Once your computer is compromised, it will go

to the fake site even if you type in the correct web address. Another technique is called "DNS Poisoning," which is when the DNS table in a server is modified so you think you are visiting a legitimate website, but you have actually been redirected to a fraudulent one. With DNS Poisoning, the attack is occurring in the DNS server, while your individual computer may not actually be compromised.



PHISHING	PHARMING
* Criminal tricks victim into providing sensitive information through email or text message * Involves a fraudulent link to a website which then attempts to gain the user's information * Is an attack directed at one person at a time * Phishing attacks are relatively easy to initiate as well as identify * Requires unsuspecting victim to click on malicious code in their inbox	* Seeks sensitive data through domain spoofing * Works by exploiting DNS system and is harder to identify than Phishing * Targets multiple victims at a time by using a technique called "DNS Poisoning." Works by infusing false info into DNS, redirecting users to illegitimate websites designed to steal data. * Spyware removal tools are useless because technically, there is no malware on the end-users' computers.

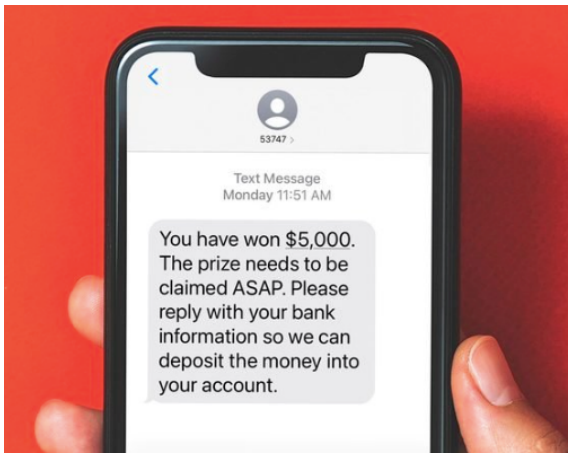
HOW TO DETECT PHARMING:

If you go to a website (especially one that you use often) and the color, look, *feel* of it seems *off,* you may be a victim of pharming and you may actually on an illegitimate website designed to fool you into giving up your data. The website URL may have a misspelling in it. (They can't use the correct spelling because that would lead the potential victim to the correct website.) Also, not

that this is a telltale sign, but fake websites will often use "http" instead of "https." (Http stands for hypertext transfer protocol. Http with an "s" added, ("https") the "s" stands for "secure.")

SMISHING

Smishing is Phishing, but with a mobile phone instead of a computer. The cybercriminal sends a text message which uses "social engineering" to obtain personal and sensitive data from the victim. They work by falsely representing that they are from a trusted, reputable source.



They often say:

* You must confirm your I.D.
* There's a problem with your account, payment information, shipping address, etc.
* "We've noticed an unusually large number of log-in attempts"
* "Warning: suspicious activity has been detected on your account"
* "Register now for "stimulus" or "refund," or "you are eligible."
* Register now for free (anything) or a coupon, discount, or something else too good to be true
* Your package has been lost, please click here for more information: http://bit.lee/900tru
* Your new Iphone has been shipped, click here for more details. (And you never bought one)
* Of course, let's not forget "you've won a prize!"

Smishing is different than Phishing and Pharming because it is more of an interpersonal scam rather than a malicious code penetration of the computing device (mobile phone rather than regular computer.)

SOCIAL MEDIA MESSAGING SCAMS

These are, of course, scams involving the use of social media. They include (but are not limited to:

* Quizzes for fun: A Facebook quiz to determine what learning style you are, or involving romance may seem harmless, but personal details obtained through intrusion can be obtained to further infiltrate your identity and finances.

*Beware fake messages from fake or hijacked profiles: Social Media cybercriminals can pose as someone you know and trust, contact you, and attempt to obtain money or personal data.
* Romance scams stemming from social media communications have increased exponentially in the past few years. Eventually, the cybercriminal asks for a phone card, wire money, or a "loan" to help with a "medical emergency."

*Sellers that fail to deliver often do business through social media. Use of reputable merchants with insurance to cover failed delivery will help prevent loss. Beware a "deal" too good to be true.

EMERGENCY SCAMS AKA "GRANDPARENT SCAMS"

There are multiple (and creative) variations of this scam, but the essence is still the same. Seniors are targets of this scam, cybercriminals prey on their family ties. The grandparent receives a frantic call from someone claiming to be their grandchild and in distress from being arrested, having a medical emergency, or some other kind of excuse to require the immediate wiring of "emergency" funds. The grandparent is conned into wiring thousands of dollars and the scammer may repeat the process, "doubling up" on the false narrative.

To avoid being scammed, be suspicious when you receive a telephone call where:
* A grandchild calls you from a far-away location.
* The grandchild says, "It's me," or "It's your grandson," or "It's your favorite grandchild."
* The grandchild is in some trouble or some type of distress.
* The caller asks for money to be wire transferred

ONLINE "MARKETPLACE" PURCHASE SCAMS

Scammers using Facebook and online marketplace sites have found creative ways to scam using that medium. In a typical Facebook Marketplace scam, the scammer would send a fraudulent check for more than the sale price of the item “to cover shipping costs” and then convince the seller to refund the overpayment. Now, scammers are convincing buyers to use Zelle for payment transactions or some other payment method where, after transfer, the payment cannot be reversed. Some methods to avoid being cheated include purchasing from a reputable website, or purchasing locally with an agreed hand-to-hand exchange in a public location.

RANSOMWARE (AND OTHER MALWARE)

This type of attack has been at the forefront of headlines throughout the country in the last few years and is fiendishly clever in its implementation. This kind of attack is as formidable as it is evil. An unsuspecting victim inadvertently clicks on an email or some kind of file with a hidden executable enclosed within. (It really is as simple as clicking on a file, innocently-disguised malware for penetration of a computer, or, even worse, a host network.)

After clicking on the malware, a message of some kind, usually with a countdown timer, pops up on the victim's computer screen, giving an instruction stating something along the lines of "Your computer is now encrypted, you must pay, or when the timer reaches zero, your data will be destroyed." The victim will find that the computer is frozen and the only part of the GUI that's usable is a button that says: "pay here." The victim is directed to pay using an irreversible method (no way to get the money back once paid), usually (untraceable) cryptocurrency, and once

paid, the "key" to repairing the infected computer is provided.

Once can easily see that if the target is a government agency with years of precious data, when faced with the choice of losing that data, or worse yet, allowing confidential information to be dispersed, the agency pays the cybercriminal.

As attorneys, we are all too familiar with a "cost/benefit analysis," and when it comes to ransomware, the cybercriminals who engage in this type of attack are usually pretty careful to make the price-point for saving the system a deal that can't be refused. If the cost is so high that the agency can't afford to lose the funds, or the agency doesn't have ransomware insurance coverage (yes, that is a thing, nowadays) then the attacker doesn't get paid and nobody wins. If the amount sought is low enough, the victim will pay to have his computer restored and chalk up the payment to experience. (And after the experience, the victim will take measures to prevent this attack in the first place, maybe measures they should have taken in the first place.)

Some consider ransomware to be a "virus," but this is not the case. These are directed attacks, not designed to be hidden, but rather to be at the forefront and can't be ignored or stopped (usually) with virus detection/protection software.

HOW DOES IT HAPPEN?

Social Engineering: Most cyberattacks have elements of social engineering, information provided with are targeted at a user's needs, wants, search patterns. Social engineering makes the attack more effective by personalizing it, making it more personal to the victim.

Spear Phishing: Is a targeted phishing attack. Examples include sending emails to members of a social interest group, or a spoofed email to employees of a company, falsely portrayed as coming from the CEO with instructions to open a specific file. "Whaling" is Spear Phishing directed at high-level executives.

Malspam: Cybercriminals send emails with imbedded malware to as many people as possible, expecting that someone invariably will click on the executable and allow penetration of the system. The rigged files might even be an attached PDF or Word document.

"Malvertising," (also known as "drive-by-download") This is malicious advertising, using online ads to distribute malware. In some instances, users can be redirected to the cybercriminals' illegitimate websites without even clicking on an ad. Criminals catalog victims' data, providing information about the users' such as searching habits, locations, information to formulate more targeted attacks. A "drive-by-download" is where the user lands on a landing page with hidden exploits, malicious code attacks the victims' system (through an exploit kit) and all of this happens in the background without the user knowing.

RECENT SCAMS TARGETING ATTORNEYS

*** Scammers pretending to be from Bar Association:** Using email spoofing, attorneys have received emails from scammers which purport to be from a state Bar association. (2020 Texas Bar case with fraudulent "gofund" me scam)

*** Legal Representation Scams:** While it is certainly helpful to utilize electronic means for obtaining potential clients, without taking necessary precautions, a lawyer can fall victim to an impersonator, or a cybercriminal with an eye on the attorney's trust account.

*** Debt Recovery Assistance Scam:** Scammer insisting that debt recovery check run through Attorney's account (cashed) and funds wired prior to check clearing.

*** Family Law Attorney Scam:** a purported ex-wife working in Asia seeks a law firm's help collecting a settlement from her "ex-husband," a United States resident. The ex-husband has a counterfeit "certified" check delivered to the law firm. If the scheme is successful, the law firm wires the client the balance of the settlement payment, after deducting its fee, before discovering the check is a fake.

*** Sally Anderson, Vice President – claims at Wisconsin Lawyers Mutual Insurance Co., (article) says:** Don't be fooled by:
* emails that are personally addressed to you;
* follow-ups to an initial email message;
* legitimate-looking referrals from another local attorney. Some lawyers routinely forward emails asking about family law matters to lawyers they know who practice in that area;
* legitimate-looking identification;
* innocent-looking subject line messages such as "collaborative family law agreement"; detailed background information; or
* phone calls that appear to be from local numbers. It is easy to fake a local area code and phone number with calling cards.

*** Attorney "Advance Fee Fraud:"** (ABA Article) A prospective client contacts you seeking representation in a dispute. You do not know the client, but he emails you background documents on the dispute and confirms the details by phone. He signs your engagement letter.

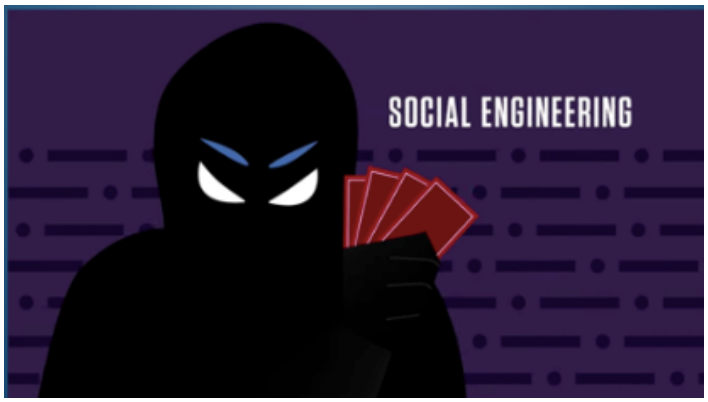
Almost immediately, the matter settles. The adverse party sends a large check, made out to you for the benefit of your client. You notify your client and deposit the check in your attorney trust account. Your client tells you that he needs the funds immediately and provides his wire information.

II. "<u>SOCIAL ENGINEERING"</u> IS USED TO ASSIST CYBERCRIMINALS IN MAKING THESE ATTACKS MORE EFFECTIVE.

"Social Engineering" is a term used to describe specific activity of cybercriminals (or advertisers) when they design attacks (or ads) for a specific person or group. The attack is

designed to appeal to the target by using the target's interests, behaviors, motivations, wants, and needs. Social engineering is based on manipulation.

kaspersky



Kaspersky (a well-known cyber-security firm) states:

"Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively. In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.
Generally, social engineering attackers have one of two goals:
Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
Theft: Obtaining valuables like information, access, or money.

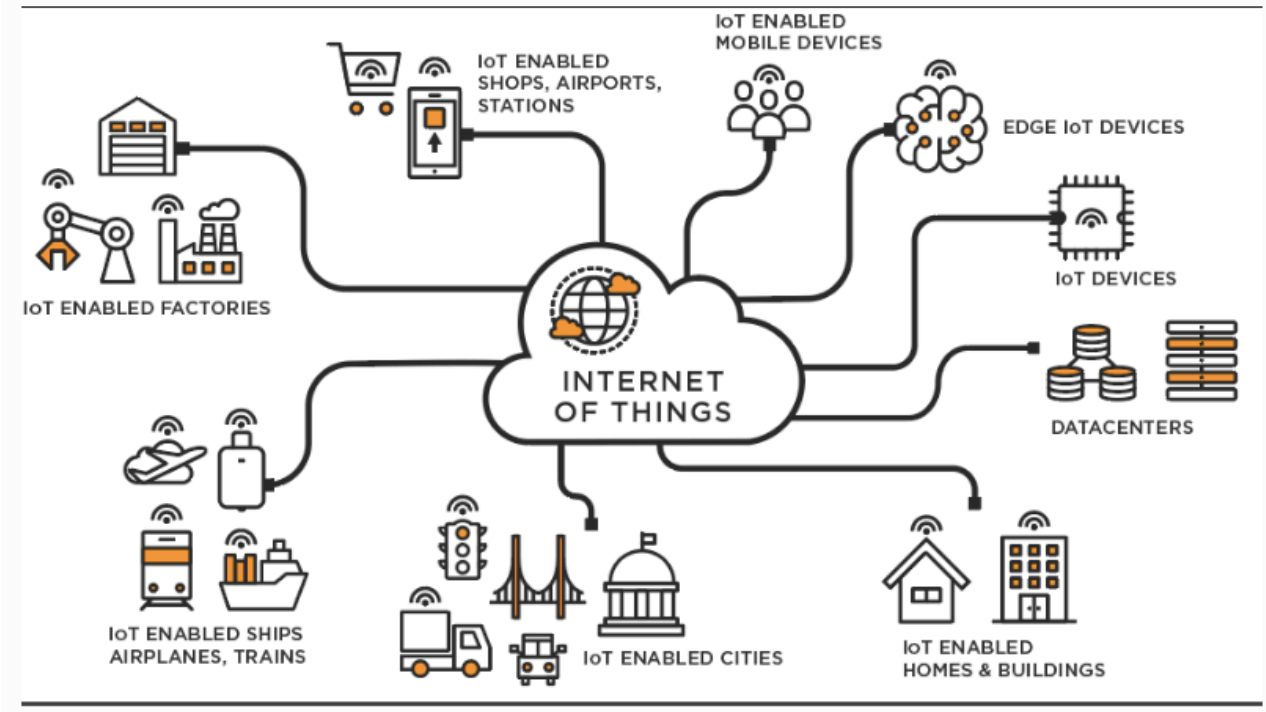
How Does Social Engineering Work?
Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.

The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

Prepare by gathering background information on you or a larger group you are a part of.
Infiltrate by establishing a relationship or initiating an interaction, started by building trust.
Exploit the victim once trust and a weakness are established to advance the attack.
Disengage once the user has taken the desired action.
This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.

It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts."

II. Beware the "Internet of Things."



II. "Internet of Things." (IoT) Proliferation of internet-accessed devices, has led to the "Internet of Things," (IoT)

Go to any department store and try to buy something that isn't "smart," and you can see that these devices are becoming the norm. We have seen "Smart Televisions," but consider the other items, things that we buy that would not normally be connected to the internet, such as refridgerators, stoves, washers, dryers, other home and kitchen appliances. Consider the "Smart Toaster."

IBM says: "The Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them."

Ask yourself the question: "Why is my toothbrush connected to the internet?" (Yes, there are "smart" toothbrushes.) The devices are watching, listening, not because they are connected to Skynet and taking over the world, it is much more nefarious. It is because the companies want to sell you things!

Your "Smart Toaster" "sees" that every day you toast an "Eggo" waffle. You can guess what happens next: you get an advertisement or coupon for those very same waffles. "How fortuitous," you think to yourself.

Your "CPAP" (sleep apnea) machine is smart, too. It's connected to the internet, supposedly so it works better.

Then you go to the dentist. (Of course, from eating too many sugary waffles.) Your dentist looks at you with those jewelry-goggle-glasses on the end of his nose and says: "your smart toothbrush says you only brush once per day. Better make it at least two."

You get a notice in the mail from your insurance carrier who says they are not going to cover your new CPAP machine because you have not been using the device correctly. It is, after all, connected to the internet, and it knows when you've been sleeping, and knows when you're awake....

Why do I really care if my Smart Toaster is listening to me? A "Smart" device is something just waiting to be hacked. If you are an attorney, and you are standing in the kitchen, talking to your client who has sensitive information, your toaster is listening, or, rather, the hacker who infiltrated your toaster with some malware during the last update, is listening.

Are you liable for costing your client millions because you unwittingly gave sensitive information by simply having a smart device that was hacked?

IV. TOOLS AND TECHNIQUES TO PROTECT YOURSELF, OR TO AT LEAST SURVIVE AN ATTACK.

I think cybercriminals don't know about us yet. If they did, I think we, as attorneys, collectively, would be screwed. Just acquiring the ability to practice law is a life-altering task, never mind staying abreast of changes in the law, in the practice, and the ever-changing techniques required for serving our clients.

We, as lawyers, are not normal people. Plumbers, food-service employees, electricians, teachers, and most of the rest of the world do not have the same pressure to protect clients that attorneys have. Attorneys have a uniquely onerous responsibility to protect our clients. As attorneys, we have a duty to protect our clients' secrets and to protect our clients' money. Both client's money and client's secrets are vulnerable to cyberattack through the attorney-client relationship.

I guarantee that right now, at this moment, there is a nondescript building in India, Nigeria, Moldova, or some other cybercriminal-hosting country where people are in a room looking for yet another vulnerable group of people who will be the target of a socially engineered phishing attack. I would confidently argue it's only a matter of time before they start attacking those of us who work in small law-firms.

Is it inevitable?

1. Do NOT focus (at least primarily, you'll make yourself crazy) on prevention. Focus on mitigation, that is, what you do afterwards.

A. Make multiple backups: Hard drives and Cloud Storage
B. Clone operating environment
C. Use VMs (if you can make yourself)
D. Updates (Windows Defender)
E. E-Wallet (type) programs
F. Preferences and settings (no cookies, no autosave logins, etc.)

The number one way to protect yourself is, of course, backing up your data. (Weekly? Monthly?)

APPLE'S BUILT-IN SOLUTION

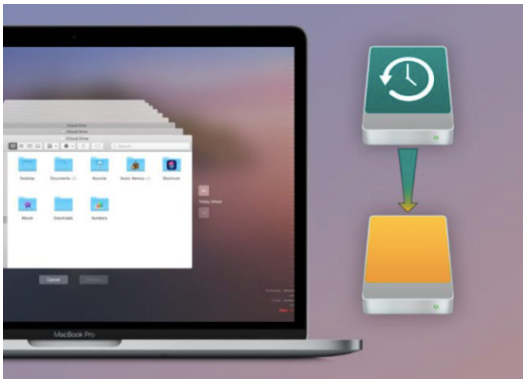
Apple Macs: OS X: Those of you familiar with Macs and OS X have the benefit of Mac's built-in software called "Time Machine." The very first time you get a portable hard-drive and run "time machine," you're going to think "this is crazy," and leave it connected overnight. (if you have a big hard-drive and lots of files, it is going to take longer. (Seriously, turn out the lights, leave the thing on and come back in the morning.)

The good news is that once a <u>full</u> "time machine backup" has been made, OS X has optimized the program to "fill in the blanks," and making new time-machine backups is a MUCH quicker process. What happens, is that the software recognizes the file additions and deletions (you made since the prior backup) and makes incremental backups based upon the changes. It does not need to make a "full" back up each time. Time Machine software has been around for over a decade and is rock-solid. The backups are separated by date and you can even restore to a specific date and time **prior** to being infiltrated or infected. The best part about OS X (and time management) is that you don't have to actually sit through the time-machine backup process. You can tell the Mac to do the time machine backup, set the computer to shut down automatically in an hour or so, (it's in settings, do NOT leave your Mac on when you are not using it) and leave for the day, knowing you'll (automatically) have a complete backup, and the computer will shut down and you can rest easy in the knowledge that your data is safe and secure.

You can even set your time machine to backup to ICloud or some other "cloud storage" solution. If you do this, however, know you'll be paying for the subscription for extra storage space, but the good news is that it is well worth the money. Whether you are using a "Google Drive," "Dropbox," "ICloud," Microsoft OneDrive, or some other service, having a cloud backup storage solution **in addition** to your physical backup (external storage device) will ensure that you are never victimized.

If you are using a Mac, spend $80 on a portable hard drive and use time- machine. Save to BOTH external hard drive AND cloud storage. You can put it on and leave for the day.

What kind of backup do we need? Just the files, or the entire computing environment?



"Drag and drop" v. "Disk Image"

When discussing backups, I'm not necessarily talking about "drag and drop" solutions per se, I'm talking about a **complete disk image.**

What's the difference? You can use file management (Finder in Mac and File Manager in Windows) for drag and drop backups if you are only concerned with files themselves. For me, I need a disk image solution to be able to restore my computing environment to pre-infiltration. There are some differences, pros and cons to each method.

Backing up files separately (Drag and Drop)	Disk Imaging Solutions
* You can pick and choose exactly the files you want to back up * Process is usually faster and easier than cloning the entire hard drive * You generally can't "set it and forget it" either Windows or Mac, there will always be name/number errors and overwrites. (This means you have to wait and watch while the backup is in progress) * If you are infiltrated you will have your files protected, but a reinstall of operating system will cost a great deal of time and energy. To restore your normal computing environment you'll have to reinstall your software programs, reset your settings, recode your passwords and license keys.	* Can't pick and choose files (for the most part), you are saving a "clone" of the entire operating environment. * Process can take a long time and can be complicated to set up, but once done, becomes much faster and easier. *Generally restores computing environment to pre-infiltration status, with some exceptions * Can set is up and let it work without you having to stand over it during entire process.

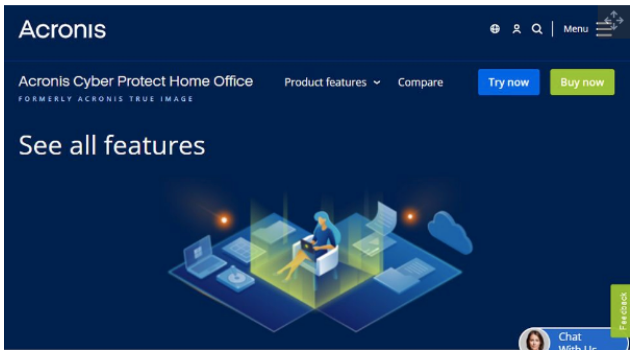
IF YOU USE WINDOWS 10 OR 11:

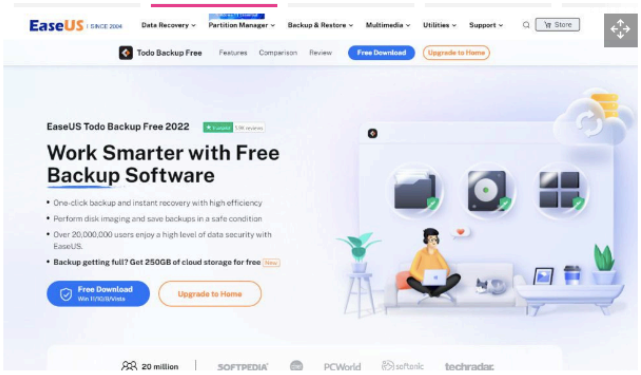
Windows: If you use conventional means to clone a back-up your hard-drive, using Windows "cloning" software, or other commercialized backup solutions, this can end up being time-consuming, almost prohibitively so.

Windows 7 had a "Backup and Restore center." Windows 10 and 11 have similar built-in solutions, but Microsoft's backup solutions are usually much more time consuming and complicated to get up and running.

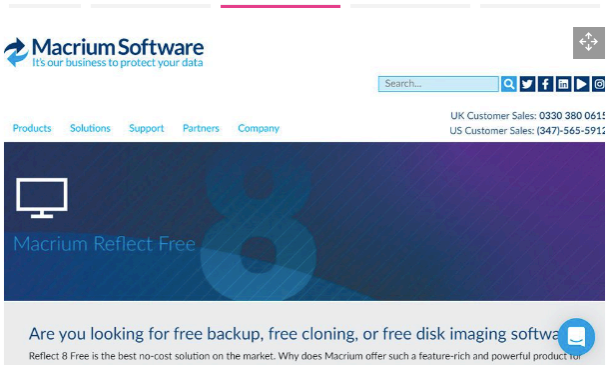
TOP FIVE THIRD PARTY SOLUTIONS (FOR CLONING ENVIRONMENTS)

For Windows, a commercial program is the easiest, most efficient way to clone a hard drive's contents and preserve your computing environment.





(Image credit: EaseUS)

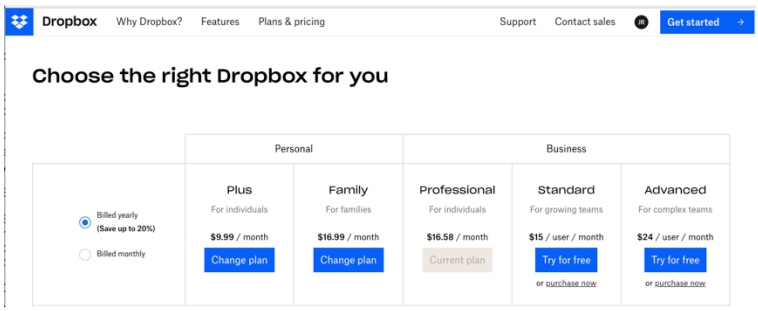


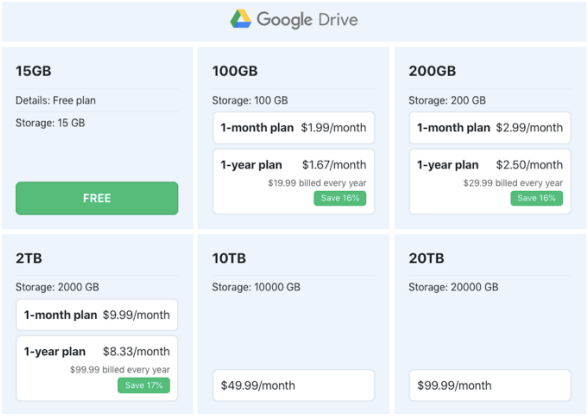
(Image credit: Macrium)

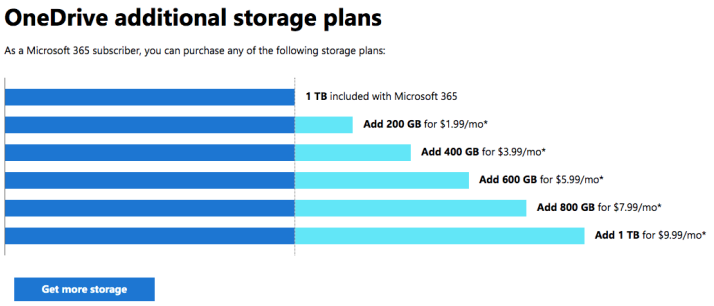
(Image credit: Paragon Hard Disk Manager)

(Image credit: AOMEI)

Backing up Files (Not the entire drive, just the files) Aside from portable hard drives, there cloud storage options:







IF YOU CHOOSE TO BACKUP YOUR DATA...

And you are attacked by ransomware, some other kind of malware, virus, worm, or other nefarious infiltrator, you won't have to worry about your data and you won't have to pay a ransom to get it back. You may need to perform a complete system wipe-down, but know that once completed, you can restore your working environment and be back up and running without further threat.

ASIDE FROM BACKING UP, SOME OTHER CONSIDERATIONS:

2. Trust Account Vulnerability

Where is your clients' money? Is it in your trust account? How much is there? What bank has your trust account? Who know the routing number? Are the login credentials stored on your Chrome browser? Do you have them written down on a legal pad or a "sticky" someplace? Does your secretary know? IS it in your secretary's Chrome browser?

QUESTIONS:

A. Do we really need to use our trust accounts? If so, how much do we need to use them?

Is it possible to practice law without the use of the trust account, or, maybe, even (very) minimal use?

For me, the small (very small) Family Law practitioner, the answer is a resounding "yes." I make my clients pay the court reporter, mediator and any other outside vendor directly. That money does not go through me. Filing fees are exact amounts given to me by my client then taken out by the clerk. If there's a way to use a third-party processor for payments, make them do it.

B. Do we need to have only one trust account? (I don't know the answer to this and can't find one. I called the hotline three times and got a different answer each time, someone, anyone help me.) Can we rotate them? Can we have a few of them and use certain ones for certain clients? Would that even help?

C. Can you change your trust account each year? Every six months? (At least change the account number if you're too lazy to go to a different bank.)

D. Tell me RIGHT NOW how long have you been using the same login and password?

How many ways is your trust account vulnerable?

I'll freely admit that my situation is different than other lawyers. My clients are folks fighting over lawn furniture, a double-wide, one of those old Ford Pintos that explodes when its hit from behind, and my clients pay me with chicken sometimes (shit up) so trust account use isn't high on my priority list.

For you, the question remains: how can you limit your trust account exposure?

3. Use a "Cybersecurity Acknowledgment, Agreement, and Waiver."

This lets your clients know that if they decide to text you "state secrets," IP, the plans to their invention or prototype, or where Jimmy Hoffa's body is buried, and you get hacked, it's on them for texting you such sensitive information.

I have attached one of these. There's also a link to download it from my website (a private URL) in: MS Word. Go here: https://www.rapkinlegal.com/emailclass

I drafted it myself and I know it could be better. If you can make it better, please do so and share with the rest of us. We are ALL going to be under attack, (someday). Let's help each other.

It's only a matter of time before that nondescript group Bangladesh, in a criminal cyber-hacking brainstorming session says: "how about Florida lawyers? I hear they have money in their trust accounts."

4. Limit putting your personal information out there.
Facebook, Instagram, Twitter, Discord, Linkedin, all are the "bread and butter" of social engineering.

Do you: Have a dog? Put pictures out there? Use the dog's name as a password?

5. Passwords SUCK.
Use an e-wallet program. Be creative. (lyrics to a song, your favorite poem, coupled with characters and numbers.)

This was on Twitter:
"My dad told me his password is: MickeyMinnieGoofyDonaldPlutoHueyLouieDeweyDublin. Because he was told his password had to contain 8 characters and at least one Capital."

3. OTHER TOOLS AND TECHNIQUES TO PROTECT YOURSELF

RANSOMWARE: You are only fooling yourself if you consider installing security software or taking precautionary measures after you've been infected. If you want to (try at least) to thwart an encrypting ransomware infection while you are in the midst of being infiltrated, you can try shutting down and disconnect from the internet. If you notice your system slowing down for no reason, try a full shut down and restart without being connected to the internet. If you are not connected to the internet, you may get some relief because the malware won't be able to communicate with the cybercriminal's servers and you might be able to get some help from a professional and at least save some of your data.

If you infected by some kind of malware, immediately disconnect everything from the internet, (in fact turn it completely off) then restart without being connected, and attempt to restore your systems. Change your passwords, and, if you are able, wipe and restore your devices.

You'll have to reset your administrator credentials, and make sure your servers are clean, but be sure not to lock yourself out of recovery. Of course, before you restore from a backup verify that you are free from any malware.

OTHER TIPS TO PROECT YOURSELF FROM A SMISHING ATTACK

* Don't open any unsolicited text message. If it says that it's from a particular company, look it up and check on your own to ensure that the identity hasn't been spoofed.

* Of course, don't open attachments or links from unknown sources.

* Look at the spelling of words in the text message, cybercriminals are known to misspell addresses, URL's etc.

OTHER TIPS TO DEFEND AGAINST PHISHING/PHARMING ATTACKS

* You can't do anything to protect yourself from being the victim of DNS poisoning as your computer is being redirected without being infected.

* Be on the lookout for suspicious emails or software or executable files that enable malware infiltration. If you are able to avoid opening a suspicious email or an email from an untrusted

source, of course that would help. Most importantly, if you have a suspicious email, do NOT click on any attachments or links contained within.

* Use of a VPN (Virtual Private Network) can also help, and reputable VPN services provide protection at an affordable price. Using a VPN will hide your IP address from websites and may even prevent cybercriminals from obtaining your personal data.

* Instead of clicking on a link in an email, put in the website address yourself, or use a bookmark. This way you know that the source is you and not an illegitimate link.

* Use a reputable ISP, reliable DNS servers, some that provide their own firewalls and protection services.

* If you are able, try to only go to websites that use "Https." (instead of "Http.")

* Check links/URL (Uniform resource Locator) for typos and misspellings

* Avoid deals that are "too good to be true," suspicious websites, and use two-factor authentication.

* Use strong passwords and change them on a regular basis. Never use the same passwords for everything and use passwords that do NOT have special meaning. For example, do NOT use the name of your dog, or your car, or your favorite rock band.

HOW TO AVOID BEING THE VICTIM OF SOCIAL ENGINEERING

* Be cautious and vigilant about putting your personal information on any social media website. The more information about you that a cybercriminal is able to obtain, the easier it will be to engineer a personalized attack.

* Use encryption for sending important data

* Avoid being hooked by any message that conveys a sense of urgency and uses high-pressure tactics.

BUT WHAT ABOUT CELL PHONES?

Video of app made to collect your data
"Permissions"
What's App, Tik Tok, etc.

Solution: get a phone just for work and put nothing on it. (T-Mobile Digits!)

WHEN ALL ELSE FAILS....

Unless you know it, don't click (or tap) on it.
Limit what is listening to you, at least in your office.
Go into preferences and take control of trackers, cookies, and other vulnerabilities.
Use strong passwords and change them on a regular basis.
Use two-factor authentication.
Always update. (they are almost always about security)
Check domain names and certificates before putting in login info.
If suspicious, switch browsers and type in the url yourself.
Don't click in links in emails.
Keep firewalls on. (And consider a reputable VPN)
Https:// is better than Http://
Limit the personal information you give out (avoid being "socially engineered!")
You will not be contacted by a bank or legitimate site which then asks for your login or other personal info.
Avoid getting hooked by pressure tactics. If suspicious, slow down, ask for help.
If you get attacked, turn everything off, pull the plugs and get help.