Attorneys and Email: Legal Implications, Ethical Issues, and Practical Consideration

Jeffrey A. Rapkin, Esq.

1st Hour CONTENTS

5 min: **Introduction**

9:35 Min: ***James Veitch email scam Ted Talk video***

25 Min: **I. Scenarios (Pages 1-3)**

20 Min: **II. What Is Email? (And How Does It Work?) (4-6)**

What Is A "Protocol?"
A. POP
B. IMAP
C. SMTP
Email Map/Diagram on How Email Works

2nd Hour

10 Min: **III. Changes in Rules of Judicial Administration Regarding Email Service, (E-Filing and SC17-882) (6,7)**

A. Rules of Judicial Administration for Computing and Extending Time i.e. 2.514(A)(4) "Last Day" Defined.
B. Changes to Rules of Civil Procedure: (From SC17-882)
C. Changes to Rules of Criminal Procedure (From SC17-882)

25 Min: **IV. Legal Implications and Ethical Considerations (7-13)**

A. Is Email A Proper Method for Communicating with Clients?
B. Privacy and Protection Considerations When Using Email to Communicate with Clients
C. Duty to Preserve Attorney-Client Privilege While Using Email to Communicate
Rules Regulating the Florida Bar: **Rule 4-1.6** Confidentiality Of Information (And Consider F.S. §90.502, Too.)
D. Duty to Protect the Confidentiality of Email Communications with One's Client
E. Will A Disclaimer Protect You?
ABA Formal Opinion 11-459 (Attached to The Materials)
F. RRTFB Ethical Rule 4-4.4 Respect For Rights Of Third Persons
G. Public Records Act Considerations

20 Min: **V. Cases and Precedents to Consider (13-18)**

A. Failure to Preserve Emails Can Lead to Sanctions
F.S. §668: Statutes: "Florida's Electronic Mail Communications Act"
F.S. §668.801: Florida's Computer Abuse and Data Recovery Act (CADRA)
F.S. §668.701: "Antiphishing Statute"
Chapter §815
B. Confidentiality of Personal Emails Sent Over An Employer's Server
C. Emailing A Proposal for Settlement: Can You? Should You? (SC17-716) January 4, 2019, Supreme Court of Florida RJA 2.516
D. Real Estate Attorney Sued In New York
E. Malware Attack on DLA Piper

3rd Hour

10 Minutes **VI. Protect Your Clients (And Protect Yourself, Too) (19-22)**

A. Google Is Watching You
5:41 Video: Google Listens to You, Too and Address Showing What Google Collects
4:43 Video: **CBC Canada Video**
B. Beware That Free App That Infiltrates Your Identity
4:43 Video: **CBC Canada Video**
C. Phishing: Watch out for Phishing! What is It?

10 Min: D. Suggestions for Passwords/Password Creation
E. Email Etiquette
1. Configure "Signature"
2. Reply to emails within 24 hours
3. Do NOT send Mail to the Wrong Address:
4. Do NOT send an email if you are angry or upset about something.
5. Don't Argue Via Email:
6. Have client sign "Electronic Legal Communication (ELC)" Acknowledgment
7. Eliminate "reply all"
8. Do NOT group text message.
9. Public Records Act considerations
10. Wait Before Sending Feature
11. Format Electronic Service
12. Consider privilege

15 Min: **VII. Crucial Imperatives (22-26)**

A. Backup, Backup, Backup
B. How to Avoid Phishing Scams
C. Other Protection Measures
Q and A and Closing remarks

Handouts/Articles
Supreme Court: SC17-882
ABA Article 11-459
F.S. §668.701 The “Antiphishing Act.”
F.S. §815 "Computer Related Crimes"
Supreme Court: SC17-716
RJA 2.515, 2.516, 2.520, 2.525, 2.530
F.S. §90.502 "Lawyer-Client Privilege"
Florida Attorney General: How to Protect Yourself: Imposter Scams
Scamwatch: Inheritance Scams
Netflix Phishing Scam
Scamwatch: Phishing
Your Account Has Not Been Hacked: For Attorneys and Law Firms

Attorneys and Email: Legal Implications, Ethical Issues, and Practical Considerations

Jeffrey A. Rapkin, Esq.

For the practicing attorney, using email to communicate with clients can be convenient, but there are dangers involved. With Fortune 500 companies being hacked on what is seemingly a regular basis, what can a small-town lawyer with minimal resources do to protect himself or herself as well as protect the interests and privacy of clients? We can safely assume that companies such as Target, Home Depot and Wal-Mart (etc) have spent hundreds of thousand dollars on cybersecurity, yet hacking has occurred, lists and information was stolen. And this type of criminal activity continues.

We all must use email for E-Filing and most of us use it for communicating with clients, other lawyers, witnesses, and any other day-to-day legal practice needs. Every time we click on "send and receive," we may risk a hacker breaking through our meager firewalls, our antivirus suites, and stealing private and protected information that we are oath-bound (as Attorneys) to protect.

The following information is compiled and designed to educate Attorneys regarding the legal and ethical hazards which accompany the use of email in a law firm, (and the practice of law) and to also provide tools for lawyers to use for minimizing risk to themselves and clients.

James Veitch Video. (9:35)

I. SCENARIOS

1. You are at the Clerk's Office (filing documents, killing time until your next hearing) and you see the computer terminals usually used for researching dockets. After you ask permission, the lady behind the glass says (she doesn't care whether) you can use the computer to check your email.

2. You are an Attorney working part time as a private practitioner and part time providing legal services to the county and you receive an email from the mayor that says:
"Hey I have a quick question. What's the difference between first degree and second-degree murder? Is the first degree where you think about it first and second is where you get really pissed off first? For that matter, is it "manslaughter" and do you go to jail if you accidentally shot someone, say a plumber, or electrician because you thought he was sleeping with your wife? I mean that and you, of course, felt afraid for your own safety and the safety of others, too."
You respond to the email and provide the legal thresh-holds (and possible sanctions) for first degree, second degree murder and manslaughter. You then go to dinner, wondering "what's that all about?"

3. You receive an email from opposing counsel (on your worst case) and it says:

"Don't worry Larry." (No, your name is NOT Larry) "We don't need to disclose any of that exculpatory evidence unless they specifically ask for it. I like to hide all those bank records and information until the last minute and maybe we can keep the judge from finding out about it at all. Also, make sure you liquidate and put it all in a safety deposit box, too."

4. You receive an email from opposing counsel (on your second to worst case) and it says: "Don't worry Larry." (No, your name STILL is NOT Larry) "I went ahead and deleted all sixteen terabytes of those emails. I also pulled the hard drives and put them in the trunk of my car. It will be fine."

5. You are working on a multi-million-dollar case and your client emails you and asks for legal advice and on how the case is progressing. You email back and there is the standard disclaimer that says: "Notice: this email communication is privileged, there is an expectation of privacy, and is for the purposes of legal advice only." You go on to say: "the case just took a very good turn for us. Please see the attached lab results. Timing is everything on when we disclose. We'll talk later about it on Tuesday at our meeting."
Then you click on "respond all" and send the email to everyone.

6. You are working in your private firm and you receive an email from a longtime client that says: "I think there might be something wrong with me. I opened the newspaper up and saw that another kid had gone to his school and shot up the place and my first thought was "good for you." Is there something wrong with me? I tried to go and see my therapist, you know the one I told you I was seeing for the past six months, but I can't find her anywhere. I'm thinking maybe she doesn't really exist at all and every time I went to see her, I must have been hallucinating, sitting in my car, drooling on myself. Someone at the unmitigated hell I like to call my daily job asked me "how's life?" My only response was that "the plot was good, but it fell apart towards the end."

7. You are an Attorney working for the Public Defender's Office and you receive an email from one of the Paralegals at the State Attorney's Office that says: "Just to be sure, you are going to see if the defendant pleads guilty, even though the victim has moved to Argentina?" Scratching the back of your head, you realize it's your case and the Assistant has sent the email to the Assistant State Attorney who has the case, and "cc'd" you as well.

8. Your client says: "You can reach me by Facebook, Facebook Messenger, and Twitter, but don't use Instagram, I don't think Instagram is secure and private."

9. You receive an email that says: "I found you on your website as I am in need of a divorce attorney. I reside full time in Bangladesh but I am also a resident of your state and I am part of the Bangladeshian Royal Family. I am in need of legal assistance to secure millions. Can you please send me a retainer?"

10. You receive an email that states: "I am in the process of selling an Helicopter (Bell Helicopters 407) to a buyer residing in your area. I need an attorney to help me draft a purchase and sale agreement for the transaction. I have attached some necessary details of the Helicopter for your review, please advise on your rate, retainer fee and forward to me your retainer agreement to sign, sales price totaling $2,250,000 USD.
I have attach the copy of the Helicopter (Bell 407) I am selling below. Find below the name of the proposed buyer for your conflict check.

11. You receive an email from the FBI. It states: "We are investigating a series of bank and wire fraud transfers relating to local attorneys trust accounts. Please click on the link below to learn more and how to protect your firm." You click on the link and are greeted by the FBI's website and an article concerning theft of Attorneys' trust accounts.

12. A client comes in to retain you for his divorce. His mother attends the meeting with her son and writes you the check. You explain privileged communications and the client requests communication by email, tells you that you can talk to his mother about "anything" and that you and he should "cc" her on all matters.

13. You receive an email from a client that says: "Hey, I know you said we could make this all go away with the right incentives. I'm prepared to color outside the lines, just as we discussed. With your guidance, I'm sure we can resolve all of these issues to my satisfaction if we apply pressure in all the right places."

14. You get an email from The Florida Bar that states: "Arrearage: Pay Your Current Member Dues or Your License will be Suspended." There is a link in the email that takes you directly to the Florida Bar.

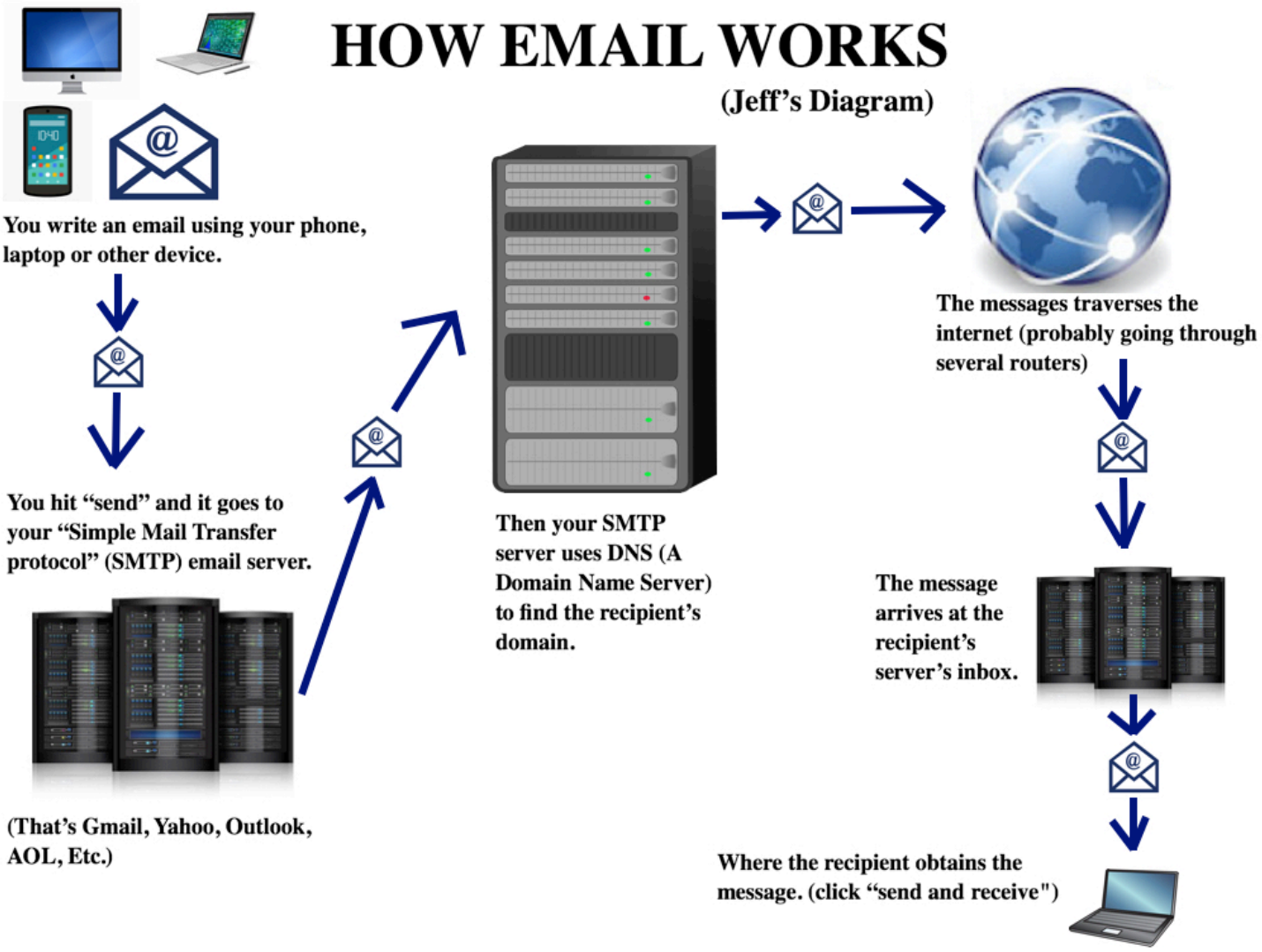
15. You are a Real Estate Attorney handling a multi-million dollar sale for a client who is selling his multi-million dollar home. At lunch, the client tells you to mail his multi-million-dollar check from the proceeds from your trust account to his home address. After lunch, however, you receive an email from him that says: "I had a great time at lunch, probably shouldn't have had that last martini. Go ahead and just wire transfer my funds from your trust account to my bank account. I don't much trust the postal service. Thanks for everything."

16. You represent Denny's in a discrimination lawsuit. You an opposing counsel settle the case and corporate provides $65,000 which you put into your trust account. You receive an email from opposing counsel that says: "Glad we could get that resolved. I forgot to ask, how did George (your son) do on his SAT's? I hope he gets into University of Tampa, he's been dying to go. Maybe he'll go to law school and go to work for our firm. LOL. Anyway, go ahead and wire the $65,000 to my client's account from your trust account. See my enclosed instructions. Good working with you and looking forward to the next one."

II. WHAT IS EMAIL? (AND HOW DOES IT WORK?)

Email was conceived simply as a method for computers to communicate with one another. In the early 1960's, ARPANET, a computer communications network created by United States Department of Defense developed a system of email transfers that relied upon the now familiar "@" sign. *Ray Tomlinson*, the man widely acknowledged to have masterminded email as we know it chose the @ symbol deliberately. According to Tomlinson "The primary reason was that it made sense. The @ sign didn't appear in names so there would be no ambiguity about where the separation between login name and hostname occurred. (*Raytheon BBN Technologies, 11 February, 2011*).

Raymond Samuel Tomlinson (April 23, 1941 – March 5, 2016) was a pioneering American computer programmer who implemented the first email program on the ARPANET system, the precursor to the Internet, in 1971; he is internationally known and credited as the inventor of email.



My diagram is a VERY simplistic diagram on how email gets from your device to the recipient. There are other factors involved, such as "Mail Transfer Agent" (MTA) software, which is used within a n Internet Message Handling System (MHS), TC/IP protocols, and other elements, which really have no bearing on our issues.

ARPANET Stands for: Advanced Research Projects Agency Network
The Advanced Research Projects Agency Network (ARPANET) was an early packet-switching network and the first network to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet.

Email communication is generally conducted via three protocols: IMAP, POP, and SMTP.

What is a "protocol?" Protocols are networking software methodology, rules and guidelines that allow your computer to link up to networks everywhere so you can send and receive email and shop on Amazon and most everything else) Your IP address, (Internet Protocol address) is just one of many protocols.

A. POP stands for Post Office Protocol. The current version is "Pop3." POP downloads the entire email into the local computer and deletes the data on the server once it is downloaded. I think POP3 is probably on its way out because of how it operates. In the past, (when computers were very big and very expensive and AOL was a thing) we all used POP3. We'd go to our computers, hit "send and receive" and our email would be pulled from a server, put onto our (huge) desktop computers and the server would not keep a copy. If you crashed your computer or accidentally deleted the email program (say, like someone trying to install the latest Lucas Arts Star Wars game but there wasn't enough room, for instance) you'd be out of luck. Unlike IMAP, under the POP3 protocol, the server didn't keep copies of your email and you'd be sunk because there was no way to get them back. POP3 is a drawback from when people used only one device to do all of their email communicating.

B. IMAP: stands for Internet Mail Access Protocol. This protocol is two-way and is used while receiving an email. When one uses IMAP, the emails will be present in the server and not get downloaded to the user's mail box and deleted from the server. (Like POP3) This helps to have less memory used in the local computer and server memory is increased and most importantly if you need to find an email, the server always has a copy. When you send and receive emails from an IMAP protocol, its downloaded (if you have a program that does that) but it is NOT deleted from the server. This is what we are all most likely using now (hopefully) and allows clients to have two-way communication with IMAP servers. IMAP is best for cloud computing and its utilization means you can use any device you want (to access email) whether it is a friend's laptop, or a terminal at the library.

C. SMTP: stands for Simple Mail Transfer Protocol. Email is sent using this protocol. SMTP contains information regarding the transmission details of an email message and is specifically used for outgoing mail. SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

III. CHANGES IN RULES REGARDING EMAIL SERVICE

All the rules, by the way, for everything, that is, can be found at Florida Bar's Website (Civil Procedure, Appellate Procedure, etc.) **https://www.floridabar.org/rules/ctproc/**

SC17-882: On October 25, 2018, the Supreme Court Amended Rules due to the utilization of Electronic Service. (SC17-882 is attached to materials.)

Of Note:

A. Rule of Judicial Administration (Computing and Extending Time)
2.514(a)(4) "Last Day" Defined. Unless a different time is set by a statute, local rule, or court order, the last day ends
(A) for electronic filing or for service by any means, at midnight; and
(B) for filing by other means, when the clerk's office is scheduled to close.

(6)(b) states: (b) Additional Time after Service by Mail. When a party may or must act within a specified time after service and service is made by mail, 5 days are added after the period that would otherwise expire under subdivision (a).
(I thought this was important because you don't get the 5 extra days for email/e-file communication.)

B. Rules of Civil Procedure: (From SC17-882) "Rules of Civil Procedure 1.170 (Counterclaims and Crossclaims), 1.260 (Survivor; Substitution of Parties), 1.351 (Production of Documents and Things Without Deposition), 1.410 (Subpoena), 1.440 (Setting Action for Trial), 1.442 (Proposals for Settlement), and 1.510 (Summary Judgment) **are amended to directly reference Rule of Judicial Administration 2.516 (Service of Pleadings and Documents) instead of referencing Rule of Civil Procedure 1.080 (Service and Filing of Pleadings, Orders, and Documents)."**

"We further amend rule 1.351 to reduce the time frame for parties to serve by e-mail a notice of intent to serve a subpoena requesting production of documents and things from fifteen to ten days. Lastly, we also amend rule 1.510 in subdivision (c) (Motion and Proceedings Thereon) to treat summary judgment evidence submitted electronically or by e-mail the same as summary judgment evidence that is "delivered," providing that while service by mail must take place at least five days prior to the day of the hearing, service by delivery, e-filing, and e-mail must take place no later than two days prior to the day of the hearing."

C. Rules of Criminal Procedure (from SC17-882): Rule of Criminal Procedure 3.040 (Computation of Time) is amended to remove the reference to subdivision (a) of Florida Rule of Judicial Administration 2.514, to conform with the amendment to that rule.

"Rule 3.070 (Additional Time After Service by Mail, When Permitted, or E-Mail) is deleted in its entirety. The rule provided its own time frames for service by mail and e-mail; specifically, it provided for an additional three days to be added to the deadline when a party had the right or was required to do some act or take some proceedings within a prescribed period after the service of a notice or other document on the party by mail or e-mail. Deleting rule 3.070 makes the Rules of Criminal Procedure consistent with the other amendments herein adopted. Computation of time in criminal proceedings is now governed by Florida Rule of Judicial Administration 2.514."

IV. LEGAL IMPLICATIONS AND ETHICAL CONSIDERATIONS

A. Is email a proper method for communicating with clients?
B. Privacy and protection considerations when using email to communicate with clients
C. Duty to Preserve Attorney-Client Privilege while using email to communicate
D. Duty to Protect the Confidentiality of E-mail Communications with One's Client
E. Will a Disclaimer Protect You?
ABA Formal Opinion 11-459 (Attached to the Materials)
F. RRTFB Rule 4-4.4 Respect for Rights of Third Persons
G. Public Records Act Considerations

Between the risks imposed by Government Workers' emails being subject to Florida's Public Records act, the possibility of the loss of protected intellectual property, to spoliation, the legal implications of an unauthorized intrusion into a law firm's servers is staggering. Some in the Appeals Judiciary are confounded by the issues imposed with the use of the internet in our daily lives. Consider the very first paragraph of the Fourth District Court of Appeals' decision in *Caiazzo v. American Royal Arts Corp.*, 73 So.3d 245 (Fla. App., 2011)

"After a great deal of judicial labor was focused on this case, but before this opinion was released, the Appellant filed a notice of voluntary dismissal. Because we believe that this case involves an issue of great public importance, we have decided not to dismiss this case and instead to release an opinion explaining our decision. We consider the issue presented in this case—the role the internet plays in a specific and general jurisdiction analysis—to be of great public importance because it involves a confusing area of the law that is mainly scattered across the federal courts and has not been addressed head-on by a Florida court. Further, because of the ever-increasing role of technology and the internet in commerce, we believe that issues relating to jurisdiction and the internet will only increase over time. Therefore, we believe it is important to address this at the earliest opportunity to provide uniformity and guidance to Florida courts and would-be litigants." *Caiazzo v. American Royal Arts Corp.*, 73 So.3d 245 (Fla. App., 2011)

A. Is email a proper method for communicating with clients?

From Texas Legal Ethics Opinion 648: (Yes, I know it is Texas and not Florida, but it is a good recitation of the major issues involved.)

"The concern about sending confidential information by email is the risk that an unauthorized person will gain access to the confidential information. While this Committee has not addressed the propriety of communicating confidential information by email, many other ethics committees have, concluding that, in general, and except in special circumstances, the use of email, including unencrypted email, is a proper method of communicating confidential information."

(See, e.g., ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof'l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008); Alaska Bar Ass'n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass'n Advisory Opinion on Prof'l Conduct, Op. 96-10 (1997); State Bar Ass'n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass'n, Advisory Ethics Op. No 97-05 (1997).

"Those ethics opinions often make two points in support of the conclusion that email communication is proper. First, the risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Second, persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. See, e.g., Alaska Bar Ass'n Ethics Comm. Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998). The statute cited in those opinions is the Electronic Communication Privacy Act (ECPA), which makes it a crime to intercept electronic communication, to use the contents of the intercepted email, or to disclose the contents of intercepted email. 18 U.S.C. § 2510 et seq. Importantly, the statute provides that "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." 18 U.S.C. § 2517(4)."

B. Privacy and protection considerations when using email to communicate with clients: While deemed proper, an attorney should take certain considerations when communicating with clients via email.

In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication. Examples of such circumstances are:

1. Communicating highly sensitive or confidential information via email or unencrypted email connections;

2. Sending an email to or from an account that the email sender or recipient shares with others;

3. Sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));

4. Sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. Sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or

6. Sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.
(Texas Legal Ethics Opinion 648)

C. Duty to Preserve Attorney-Client Privilege while using email to communicate:

Rules Regulating the Florida Bar: RULE 4-1.6 CONFIDENTIALITY OF INFORMATION:
(a) Consent Required to Reveal Information. A lawyer must not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.
(b) When Lawyer Must Reveal Information. A lawyer must reveal confidential information to the extent the lawyer reasonably believes necessary:

(1) to prevent a client from committing a crime; or
(2) to prevent a death or substantial bodily harm to another.

Also consider: (e) Inadvertent Disclosure of Information. A lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

ABA Model Rule of Professional Conduct 1.6., states in part that a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, or the disclosure is impliedly authorized in order to carry out the representation. (with certain exceptions, of course.)

From comment in RRTFB 4-1.6: "A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation."

"The principle of confidentiality is given effect in 2 related bodies of law, the attorney-client privilege (which includes the work product doctrine) in the law of evidence and the rule of confidentiality established in professional ethics. The attorney-client privilege applies in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source."

(Still in comment section of RRTFB 4-1.6)
"Acting Competently to Preserve Confidentiality:
Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 4-1.1, 4-5.1 and 4-5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (e) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to

represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

AND consider F.S. §90.502: "(c) A communication between lawyer and client is "confidential" if it is not intended to be disclosed to third persons other than:
1. Those to whom disclosure is in furtherance of the rendition of legal services to the client.
2.Those reasonably necessary for the transmission of the communication."

D. Duty to Protect the Confidentiality of E-mail Communications with One's Client: (ABA Formal Opinion 11-459)

(11-459 is so informative, I have attached it to these materials)

11-459 addresses the use of electronic communications and whether clients may have a reasonable expectation of privacy when using such forms of communication. The opinion notes that attorneys should instruct clients to avoid using workplace devices or workplace computer systems for sensitive communications between lawyer and client. According 11-459, the duty of a lawyer to advise the client about the risks involved arises as soon as the lawyer knows (or reasonably should know) that the client is likely to send or receive substantive lawyer-client communications via electronic means "where there is significant risk" that the communications will be read by a third party.

(From You Told a Lawyer Something, or Copied Them on an Email … Privileged or Not? By Anthony Argiropoulos, Gary W. Herschman & Scheherazade A. Wasty on April 23, 2018) "Simply put, just telling a lawyer something, or copying a lawyer on an email, does not make the conversation or email privileged. Not all communications with an attorney are privileged from disclosure under the attorney-client privilege. The reality is that a communication (i.e. emails, correspondence, oral communications, etc.) will only be privileged when the subject communication meets certain criteria, and it is confidential (meaning that it is not shared with non-attorney/non-client third parties).

In order for the privilege to apply to the communication itself, the "primary purpose" of the communication must be to seek or provide legal advice. In other words, a communication is not privileged if it does not: (1) request legal advice or (2) convey information reasonably related to a request for legal assistance. Thus, asking an attorney about investment advice or other non-legal issues is NOT privileged. Moreover, having a discussion (or email exchange) with an attorney, where others are present (or included) is NOT privileged."

What about Attachments to emails?
(From: Developing Issue: Attachments to Privileged Emails Not Necessarily Privileged By Todd Presnell, January 29, 2015) "The attorney–client privilege protects email communications between a client and his attorney, including communications between an employee and his company's attorney, when the email is confidential when sent, kept confidential thereafter, and is for purposes of soliciting or receiving legal advice. Many lawyers,

outside counsel and in-house counsel alike, assume that an email meeting these criteria means that attachments to the email necessarily receive the same protection.

Courts are increasingly challenging that assumption. Federal and state courts are looking beyond the email to determine whether the attachment independently meets the criteria to support application of the attorney–client privilege. Courts have held that attachments to emails "must independently earn that protection." AM General Holdings, LLC v. The Renco Group, LLC, 2013 WL 1668627 (Del. Ch. Ct. Apr. 18, 2013). They recognize with increasing regularity that email attachments can be produced independently of the cover email. Muro v. Target Corp., 2006 WL 3422181 (N.D. Ill. Nov. 28, 2006)."

E. Will a Disclaimer Protect You? Attorneys can enclose confidentiality disclaimers in their emails, in the hopes that a reviewing judge (you know the one who is dealing with the grievance and/or lawsuit) might agree that the attorney (using a disclaimer) has taken reasonable steps to protect the confidential information of clients.

Ever see this before?
"IMPORTANT DISCLAIMER: This email does not create an attorney-client relationship."

Have you ever seen this?
"The information transmitted by this email is intended only for the person or entity to which it is addressed. This email may contain proprietary, business-confidential and/or privileged material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, reproduction or any action taken in reliance upon this message is strictly prohibited. If you received this in error, please contact the sender and delete the material from all computers."

How about this?
"CONFIDENTIAL: ATTORNEY-CLIENT PRIVILEGED; ATTORNEY WORK PRODUCT: Emails and attachments received from us may be protected by the attorney-client privilege, as attorney work-product or based on other privileges or provisions of law. If you are not an intended recipient of this email, do not read, copy, use, forward or disclose the email or any of its attachments to others. Instead, immediately notify the sender by replying to this email and then delete it from your system. We strictly prohibit any unauthorized disclosure, copying, distribution or use of emails or attachments sent by us."

Do these really help?
I don't think they do. (which is why I don't include them myself.) Unlike with a contract that requires mutual agreement, the recipient doesn't need to agree to allow the enforcement of the attorney-client privilege. It is unilaterally asserted. What do you think?

F. RRTFB RULE 4-4.4 RESPECT FOR RIGHTS OF THIRD PERSONS: "(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent must promptly notify the sender."

Comment states: "Subdivision (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an e-mail or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that a document or electronically stored information was sent inadvertently, then this rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures."

Comment also states: "Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return the document or delete electronically stored information is a matter of professional judgment ordinarily reserved to the lawyer. See rules 4-1.2 and 4-1.4."

G. Public Records Act Considerations:
Consider F.S. §119.011(12)"Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."

Is there a reasonable expectation of privacy concerning the communication?
A. Not if using a government issued computer and a government issued email address, you would be subject to the Public Records act and have to turn it over.
B. What if your government email is kept by private password?
C. What if you are a private person using a terminal subject to FS 119?

V. CASES AND PRECEDENTS TO CONSIDER

A. Failure to preserve emails can lead to sanctions
B. Confidentiality of personal emails sent over an employer's server
C. Emailing A Proposal for Settlement: Can you? Should you?
D. Real Estate Attorney Sued in New York
E. Malware Attack on DLA Piper

A. Failure to preserve emails can lead to sanctions: (From "Law 360," January 4, 2017, By Carolina Bolado) "In a Dec. 29 decision, Judge Bronwyn Miller granted Progress Residential LP's motion for spoliation against Erik Wesoloski and his company Title Capital Management LLC for destroying 1.4 terabytes of data in September 2013, shortly after Progress filed suit accusing Wesoloski, who had been hired to handle due diligence of foreclosure sales, of manipulating data in order to inflate his commission."

"TCM and Wesoloski had a duty to preserve the electronically stored information, yet directed its destruction, and then failed to disclose to opposing counsel and the court the fact that it no

longer existed," Judge Miller said. "Only one conclusion may be gleaned: the evidence was critical to establishing plaintiff's claim and equally compelling evidence may not be garnered."

F.S. §668: Statutes: Note: Florida has "Florida's Electronic Mail Communications Act" and it can be found at F.S. 668.60 through 668.610, but it's no help for lawyers. In a nutshell, it makes spam (junk email) illegal.

F.S. §668.801: Florida's Computer Abuse and Data Recovery Act (CADRA), codified at §668.801, Fla. Stat., et. seq., is Florida's Data Protection Law.

F.S. §668.701: "Antiphishing Statute"

Chapter §815: Also, **Chapter 815** covers "hacking" related crimes, mostly felonies, includes hacking to destroy data, trade secret hacking, etc.

B. Confidentiality of personal emails sent over an employer's server: (From "How private are personal emails – part III: Florida district court finds no attorney-client privilege for email communications at work" Kramer Levin Naftalis & Frankel LLP)

"The Florida court's approach to the confidentiality of personal email at work drew directly from the Asia Global Crossing opinion. That decision equated personal emails sent from a work email account with general hard copy files kept at the workplace, stating that "sending a message over [an] email system [is] like placing a copy of that message in the company files. Short of encryption, . . . [e]mails [can] be reviewed and read by anyone with lawful access to the system." Asia Global Crossing, 322 B.R. at 259. Following this reasoning, the Florida District Court imposed an extremely high burden for establishing the confidentiality of personal emails sent over an employer's server. The New York Supreme Court has adopted a similarly strict approach. See Scott v. Beth Israel Medical Center, 2007 WL 3053351 (Sup. Ct. N.Y. Co. Oct. 17, 2007); see also How Private Are Personal Emails?, Electronic Discovery Update, Mar. 2008, available at http://www.kramerlevin.com."

C. Emailing A Proposal for Settlement: Can you? Should you? Wheaton v. Wheaton, SC17-716) January 4, 2019, Supreme Court of Florida: (In attachments)

"The conflict issue presented is whether proposals for settlement made pursuant to section 768.79, Florida Statutes, and Florida Rule of Civil Procedure 1.442 must comply with the email service provisions of Florida Rule of Judicial Administration 2.516."

"Respondent, Mardella Wheaton, sued her ex-daughter-in-law, Petitioner, Sandra Wheaton, for unlawful detainer. Petitioner served a proposal for settlement on Respondent via email. Respondent received the proposal but did not accept it.
The trial court granted Petitioner's motion for summary judgment.1 Petitioner then moved to enforce her proposal for settlement and to collect attorney's fees."

"Section 768.79, Florida Statutes ("Offer of judgment and demand for judgment"), "provides a sanction against a party who unreasonably rejects a settlement offer."

Section 768.79 is implemented by Florida Rule of Civil Procedure 1.442 ("Proposals for Settlement"). The rule also states that a proposal "shall be served on the party or parties to whom it is made but shall not be filed unless necessary to enforce the provisions of this rule." Fla. R. App. P. 1.442(d).

The relevant portions of rule 2.516 provide:
(a) Service; When Required. Unless the court otherwise orders, or a statute or supreme court administrative order specifies a different means of service, every pleading subsequent to the initial pleading...
(b) Service; How Made. When service is required or permitted to be made upon a party represented by an attorney, service must be made upon the attorney unless service upon the party is ordered by the court.

(1) Service by Electronic Mail ("e-mail"). All documents required or permitted to be served on another party must be served by e-mail, unless the parties otherwise stipulate or this rule otherwise provides. A filer of an electronic document has complied with this subdivision if the Florida Courts e-filing Portal ("Portal") or other authorized electronic filing system with a supreme court approved electronic service system ("e-Service system") served the document by e-mail or provided a link by e-mail to the document on a website maintained by a clerk ("e-Service"). The filer of an electronic document must verify that the Portal or other e-Service system uses the names and e-mail addresses provided by the parties pursuant to subdivision (b)(1)(A).
(Emphasis added.)

The rule goes on to provide the following formatting requirements:
(i) All documents served by e-mail must be sent by an e-mail message containing a subject line beginning with the words "SERVICE OF COURT DOCUMENT" in all capital letters, followed by the case number and case style of the proceeding in which the documents are being served.
(ii) The body of the e-mail must identify the court in which the proceeding is pending, the case number, the name of the initial party on each side, the title of each document served with that e-mail, and the name and telephone number of the person required to serve the document.

(iii) Any document served by e-mail may be signed by any of the "/s/," "/s," or "s/" formats.

(iv) Any e-mail which, together with its attached documents, exceeds the appropriate size limitations specified in the Florida Supreme Court Standards for Electronic Access to the Court, must be divided and sent as separate e-mails, no one of which may exceed the appropriate size limitations specified in the Florida Supreme Court Standards for Electronic Access to the Court and each of which must be sequentially numbered in the subject line. Fla. R. Jud. Admin. 2.516(b)(1)(E)(i)-(iv).

Ruling: "From the plain language of section 768.79 and rule 1.442, neither require service by email. The procedure for communicating an offer of settlement is set out in section 768.79(3), Florida Statutes (2018), which states:
The offer shall be served upon the party to whom it is made, but it shall not be filed unless it is accepted or unless filing is necessary to enforce the provisions of this section.

(Emphasis added.) The statute only requires that the offer be served on the party to whom it is directed and not be filed with the court but does not require service by email.

Similarly, subdivision (d) of rule 1.442 outlines the procedure for communicating a proposal for settlement to the opposing party.

"Accordingly, based on rule 1.080's plain language, rule 2.516 would not apply to proposals for settlement made pursuant to section 768.79 and rule 1.442.

The plain language of section 768.79 and rule 1.442 do not require service by email. Moreover, because a proposal for settlement is a document that is required to be served on the party to whom it is made, rule 2.516 does not apply. Accordingly, the Third District erred in affirming the trial court. Accordingly, we quash Wheaton, approve Boatright, McCoy, and Oldcastle, and remand for proceedings consistent with this decision."

(Also Attached to Materials: RULE 2.516 SERVICE OF PLEADINGS AND DOCUMENTS, RULE 2.525. ELECTRONIC FILING, RULE 2.530. COMMUNICATION EQUIPMENT)

D. Real Estate Attorney Sued in New York: (From "Uptime Legal Systems" and Law 360) A couple hired a real estate attorney to assist with closing on a $19.4 million Manhattan co-op. The attorney, the couple alleged, was using AOL for her practice's email. She did not have any basic security addons to protect her account, such as two-factor authentication. Moreover, her computer itself was poorly configured and had malware on it, enabling thieves to access her passwords and files. You can probably see where this is going. Hackers posing as the lawyer asked that the clients wire about $1.9 million as a deposit to a specified account.

E. Malware Attack on DLA Piper: (From "Cybersecurity and the Lawyer's Standard of Care" Joseph Salvo and Brian Middlebrook – May 22, 2018)
"The well-publicized June 2017 "Petya" malware attack on DLA Piper shut down the firm's email, phone systems, and operations for three consecutive days, and before being reconnected to the firm's network, all computers and devices had to be inspected and cleared. Jeff John Roberts, "Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear," Fortune (June 29, 2017). In addition, in December 2016, three individuals were charged with hacking into at least seven law firms in 2014 with the intent of obtaining inside information about prominent merger and acquisition deals. These hackers obtained 40 gigabytes of confidential information over the course of 8 days, which they used to purchase shares of stock, which yielded a profit in the amount of $4 million. In 2016, the Federal Bureau of Investigation warned of a Ukraine-based Russian hacker known as "Oleras" who solicited other hackers to attack 48 top Chicago law firms, targeting company mergers and acquisitions information through phishing schemes. In the same year, Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP, and other major law firms were penetrated by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies. Yet, in 2015, the ABA Legal Technology Survey Report found that almost half of the 90,000 private practice attorneys polled said their firms have no data breach response plan in place. By 2017, the ABA

TECHREPORT found that 22 percent of respondents overall reported that their firms had experienced a data breach at some time—up from 14 percent in 2016 and an 8 percent increase over the prior four-year average."

"While ethical rules, common law, contracts, and industry-specific laws and regulations have long required attorneys and law firms to protect confidential client information, cyber threats and attacks have changed the manner in which firms are required to protect that information. Attorneys are expected to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. Indeed, depending on a multitude of factors, including the practice and size of a firm, it may now be incumbent upon law firms to monitor network activity, review IT reports, and perhaps employ a chief information officer (CIO) in developing, implementing, and maintaining appropriate cybersecurity programs. Failure to take these precautions and affirmative actions can have dire consequences, including claims for legal malpractice."

"How to Avoid Claims: While the duty of a lawyer to protect confidential client information is sacrosanct, in the digital age, this obligation undoubtedly extends to taking affirmative steps to prevent the unauthorized access of client information. Law firms must be aware of the risks of these attacks and create a protocol to prevent them. The first step requires evaluating the type of information that the law firm possesses in order to determine the necessary protocol to put in place. Law firms' servers hold valuable information, such as business intellectual property, medical records, bank records, and government secrets, which makes firms a prime target for hackers looking for information that they can monetize. Law firms also need to evaluate vulnerabilities in their systems and create a data security plan that speaks to every member of their team. This begins with effective employee training and education on a continuous basis. Given the evolving nature of the cyber-attacks and development of technology, annual training is not enough. Employees should be educated on how to handle sensitive data securely, which should be tailored to the specific needs of each individual firm, depending on the type of data that the firm possesses. For example, if the firm routinely possesses sensitive medical information, all employees should be educated on how to handle, receive, and transmit this information in accordance with the firm's security plan as well as federal and state regulations related to the Health
Insurance Portability and Accountability Act. This education also should include how to detect cyber attacks (e.g., a phishing email) and what to do in the event that an attack is perceived or actually occurs."

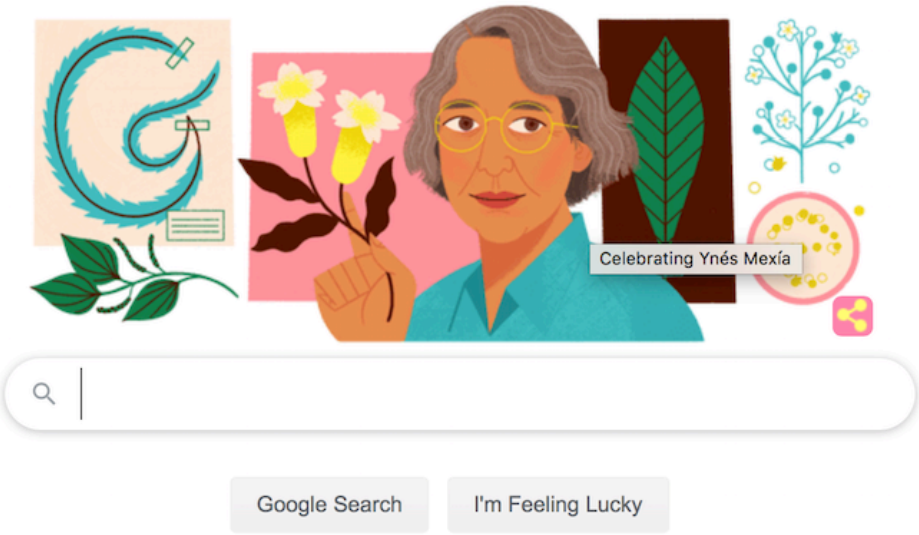
"Other safeguards and protective measures include continuous maintenance of operating systems and software programs; installation of antivirus and firewalls to prevent common malware infections; conducting third-party vulnerability scans, penetration tests, and malware scans; and ensuring that the firm's protective measures
extend to its remote access programs (e.g., Citrix, iTwin, Remote Control) for
employees who use remote access. Many firms have begun to develop "cybersecurity incident response plans," which strategically identify the protective measures that the firm has in place, what to do in the event of an attack, and longterm and short-term plans for updating the program overall. In addition, firms have appointed "cybersecurity information officers" responsible for implementing and overseeing these plans.

VI. PROTECT YOUR CLIENTS (AND PROTECT YOURSELF, TOO)

A. GOOGLE IS WATCHING YOU: Big brother isn't watching you. Google is watching you. Do you use Google?
Have you ever seen this when you open up a Google Search page?

Occasionally there will be something with the "Google" like a famous person's birthday or holiday, or event.

Like this, for example.



That's nice and all.
Now look at this next one. I went to work on my birthday, which, contrary to my mother's opinion, is NOT a national holiday and saw this:

It was meant probably as a nice thing for Google to do, but it felt creepy. Now I am starting to wonder what Google knows about me.

WEB ADDRESS TO FIND OUT WHAT GOOGLE KNOWS ABOUT YOU:
Make sure you login on Chrome or whatever, then go to:

http://www.google.com/settings/ads/

Show video on what this is: 1:04

GOOGLE **LISTENS** TO YOU, TOO.

Google Listens video (5:41)
---> Google ---> (go to the little colored dot)
---> Click on "Google Account"
---> (On the left) Click on "Data and Personalization" (It looks like a switch.)
---> Click on "Voice and Audio Activity"
---> Click on "Manage Activity"

You can now review all the things Google has that you have said. You can filter them by date. It seems to keep everything.

B. Beware That Free App that infiltrates your identity: CBC Canada Video: Journalist creates free app (a Horoscope app) and sees how easy it is to get someone's information.

Video CBC Canada Video: 4:43

C. Phishing: is a technique used by cybercriminals to acquire your personal information (such as credit card numbers or login credentials) by sending an email that is designed to look just like it came from a legitimate source but is intended to trick you into clicking on a malicious link or downloading an attachment potentially laced with malware.

Malware: is short for **malicious software,** and is software that is designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. Malware is a general term used to describe any kind of software or code specifically designed to exploit a computer, or the data it contains, without consent.

"Google for Education" Phishing Video: 3:13

D. Suggestions for Passwords:

Ewallet? Dashlane?

I use the "favorite Song" method.

1. Do you have a favorite song?
2. Does anyone know it is your favorite song?

3. You type the sentence as if you were typing out the lyrics, including proper capitals and spaces. You can decide that the only punctuation can a period at the end, exclamation point, or whatever you prefer, so long as you are consistent. (What did I use? Period? Exclamation point?)
4. Contractions can be reduced to whole words, if easier.

Examples:

Sing us a song, you're the piano man.
Her name was Lola, she was a show girl.
Hello darkness, my old friend.
I come home in the morning light.
Searching for my lost shaker of salt.
You can check out anytime you like, but you can never leave.
If you like Pina Coladas, and getting caught in the rain.

E. Email Etiquette:

1. Configure "Signature" so your client will be able to easily find your information.
Just use your name. Most email systems have an easy-to-use automated signature block. Use it to eliminate the risk that you'll forget to include basic information like your name, address, and telephone number. Some Attorneys add a privacy notice or legal disclaimer.

2. Reply to emails within 24 hours (avoid grievance for failure to communicate) Try to reply within 24 hours. If the matter is complicated, send an acknowledgment and let the person know when to expect a response. Otherwise, the client is left to speculate on whether any response is coming, or if you even care about his or her case.

3. Do NOT send Mail to the Wrong Address: The auto-complete function on email systems is a great convenience, but it increases the risk of sending an email to the wrong recipient. This could be no more than a minor embarrassment, but in some cases, it could amount to professional negligence. Don't accidentally email confidential client communications to opposing counsel or another client.

4. Do NOT send an email if you are angry or upset about something. Wait at least a couple of hours to formulate a response. You will realize that it is easier to think clearly when you aren't angry about something.

5. Don't Argue Via Email: Remember: When people speak face to face, facial cues and vocal tones help everyone to fully understand the communication taking place. In an email, it is often easy to misread a person's intent, and respond inappropriately.

6. Have client sign "Electronic Legal Communication (ELC)" Acknowledgment explaining what the rules are pertaining to privilege, confidentiality, and email.

7. Eliminate "reply all" (I mean turn that thing off so it's not even accessible!)

8. Do NOT group text message. (really)

9. Public Records Act: Be cognizant of Public Records Act considerations

10. Wait Before Sending Feature: Use setting that pauses sending email for five minutes. (in case you want to take it back)

11. Format Electronic Service: Be sure to format electronic service in accord with **R.J.A. 2.516.** (You can set this chart up as a signature to include.)

12. Consider privilege while formulating messages.

VII. CRUCIAL IMPERATIVES

A. Backup, backup, BACKUP: First, and foremost, it should not have to be said that every single one of us must utilize some kind of backup procedure to ensure that our information is always safe, secure, and available should a computer disaster occur. The Mac operating system has something called "Time Machine," which creates an entire snapshot of your hard drive. Some time ago, after an unfortunate incident which landed my 13 inch Macbook Pro into a bathtub filled with soapy water, (don't ask) I was able to completely restore the entirety of my software, data, and settings onto a new computer using a Time Machine backup. Windows users have access to similar tools and software. I have used "Winclone" myself to assist a friend in maintaining backups of his Windows computer.

Right now, this very minute, ask yourself: what would happen if your computer took a bath? Do you have a backup? If you haven't backed up your data at least once per week, you are only fooling yourself.

"Cloud" based backups: I pay two hundred dollars per year to "Dropbox." (I get 2 Terabytes per year for this) I save all of my files into the Dropbox and it syncs with my computer automatically.

The good: I can access my files from anywhere and with any device I choose.
The bad: A person bent on my destruction can access my files from anywhere and with any device he/she chooses, that is, if I am not careful with my password.

If you are meticulous with your passwords, then a Dropbox, Google Drive, Microsoft Onedrive, or any of the others are a good option for securing data.

B. How to Avoid Phishing Scams:

1. Look First: Take a moment to examine an email before opening it. Look for signs of impropriety, i.e. misspelled words, return email addresses that seem off, misspellings, bad grammar, etc.

Take measures to screen your email. Remember, a phishing email is designed to trick you into opening or replying to the message.

2. Don't talk to strangers: If you don't know who the email is from, don't open it. Sometimes you might want to even avoid opening an email that is purportedly from someone you know, if it looks suspicious. Remember there is malware in existence which can read your addresses and contacts from your computer and use one of them to send you an email.

3. Avoid suspicious attachments: If there is an attachment, only open it if you expected to receive it, even if you know who sent the email to you. It might be prudent to text or call the sender to ensure they sent you an email with an attachment.

4. If you open one by accident: If you accidentally open an email (before realizing it was a trap): options include: Close it out, don't accept anything. You might get lucky by saving your work and holding down the power button, shutting the computer down withOUT clicking anywhere near the suspicious email. When the computer reboots, you might be ok.

5. Use a workaround: If an email is purportedly from a company or governmental agency, use a workaround. Instead of clicking a link which is embedded in the email, (and which might be a trap) close the email, open a search engine such as Chrome, Firefox, or Safari, or whatever you use, and use that to go to the web address of the agency or company that has allegedly sent you an email.

6. Never give information: never give any personal, financial, or identifying information about yourself. Legitimate companies and legitimate governmental agencies like the IRS will not take information from you via an email message.

C. Other Protection Measures:

1. Downloading files from websites which purport to provide you with trial software, or "freeware" can expose your computer to Malware, Viruses, and Ransomware. Only obtain downloads from reputable sources.

2. Email Filters: almost every single email program whether it is cloud-based or installed locally onto a computer's hard drive contains an email filter program. It might be worthwhile to familiarize yourself with the tools provided to assist your cybersecurity and risk management efforts. I personally do not use these (sometimes to my own detriment) because I find that important emails will sometimes get stuck in a "spam" folder. They are out there for you to use, should you choose to use them.

3. Threat detecting and antivirus software: There is a great deal of anti-virus software and threat detection tools that are available to help you protect your data. You've probably heard of the more reputable companies before. Names such as Norton, McAfee, Kaspersky, and AVG should be familiar to you. Many have free options, and most have a subscription service which is usually not too expensive. Keep your anti-virus software updated, too. Anti-virus and firewall software are designed to prevent harmful software from installing on your computer, and can fix

breaches in your Internet security. Firewall software also helps protect your privacy on the Internet and blocks unwanted sources from accessing your computer.

4. Use secondary email addresses: In some instances, you might be able to limit your exposure if you use secondary email addresses. It might be a good practice to have an email address which is specifically for work and an email address which might be for shopping, communicating with Facebook, etc.

5. Keep your software updated: It is a drag to have to contend with what can feel like constant interruptions, freezing your operating system, leaving you to sit and wait unproductively while Microsoft puts more code onto your hard drive. If you actually look at what's being installed most of the time they are called "security updates," and are designed to protect your systems integrity. Windows 10 has settings that allows you plan in advance when updates are installed. I do not recommend leaving your computer always on, but once in a while, leaving it on overnight for updates to install ensures that a clean operating system is waiting for you in the morning.

6. Use Encryption and Two-Factor Authentication: Much like updates, using encryption and two-factor authentication might seem like a pain, but are well-worth the effort.

From Wikipedia: "Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism -knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication."

7. Consider Cybersecurity Insurance: Typically, a cyberattack is not covered under most malpractice insurance policies. Cyber insurance generally covers your practice's liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records.

8. Risk Management involves Risk Assessment: Conduct a risk assessment of all your devices, including computers, tablets, phones, etc. and assess the sufficiency of your current safeguards. Evaluate existing firewalls, antivirus software and other security measures, and take all necessary protection measures.

9. Don't turn off auto-lock: It may be a pain to have to punch in a password every time you come back from a break or go to the bathroom, but it is necessary. Configuring your computer to turn off after two minutes of inactivity will help ensure no one besides you is at your computer helping himself. You can also use "Windows Hello" which opens your computer with facial recognition or a fingerprint, and Macs will also open with an Apple Watch.

10. Don't Store Work at Home: Your office is probably more secure than your home. If you bring work home from the office, bring it back. Storing client or sensitive data on your home computer could lead to a disaster.

11. Scrub Machines: Most copy machines, scanners, and other devices sometimes keep the last few instances of use in memory. Protect your clients by deleting those files. Also, put bluetooth

devices in “non-discoverable” mode, or protect pairing with passwords and pair with other devices only when in a trusted location.

12. Be careful with online profiles: The more a hacker knows about you, the easier it is for him or her to obtain useful information for a cyberattack. What does Apple ask for when you have forgotten your password? Your first pet's name? Your father's middle name? The first beach you visited? If any of this information is on your Facebook page, you may be doing yourself a disservice.

13. Remote Wiping Software: This is a tool that comes with Macs. There are other programs available which accomplish the same tasks. Being able to remotely wipe or lock your device if it is lost or stolen is invaluable.

14. Don't Work from Starbucks: You might like a cup of coffee and to sit at one of the tables with a laptop. You can if you want to, but I doubt any Public Wifi is secure.

We don't have to be terrified when we sit down to read and respond to email, but it might be a good idea to at least be a little apprehensive. A person who breaks into your home to steal your possessions might stand a good chance of getting caught. There are fingerprints to be found, physical evidence, witnesses, etc.

A faceless evildoer in a foreign country sitting behind a two-hundred dollar laptop can clean out your savings account in a matter or moments and his or her risk is minimal. Just as a person might get an alarm system for his home (or a very big and angry dog) you too, can take preventative measures to protect your "cyberidentity."

Using proper tools and software, you won't completely eliminate your exposure, but you can certainly make it as difficult as possible to get scammed or worse yet, to expose a client.

Jeff Rapkin, 2019

Jeffrey A. Rapkin, Esq.

Supreme Court Certified Circuit Civil and Family Mediator

(941) 916-4096
Fax:(888) 713-3146
email@rapkinlegal.com
www.rapkinlegal.com

Mailing Address: P.O. Box 510727
Punta Gorda, Fl. 33951-0727

Office: 18245 Paulson Drive
Port Charlotte, Fl. 33954

Who Am I?

As a solo practitioner hell-bent on finding ways to streamline the mundane tasks involved with the practice of law, I have inadvertently become an expert in computers, their workings, and, of course, the operating systems. I grew up with computers, video games, and took classes as a teenager and in college to learn (the oldies) Objective-C, C, C++, Swift, Cocoa API, and Unix which, in and of itself, helped me to realize I didn't have what it took to make a career of it. Switching gears, I studied law, but also maintained my love for computers, computer engineering, and how such technology can be used to automate the practice of law.

My foremost build is a fifteen-inch Macbook Pro that I put together from various parts found throughout the internet. It has four (yes four) terabytes of hard drive space because I was able to pull the dvd drive, install a "data doubler" caddy and put a 2tb Sata ssd in, along with the standard hard drive, which I replaced for a second 2 tb hard drive. With this device, I could operate the standard Mac Os X, Full Windows 7 (and then 10 through a bootcamp partition) and I could run Linux Ubuntu (through Parallels) alongside with Os X.

I have 2 IPads hanging on my wall, (one is very old), I have a third IPad, which is the very first one ever made (sentimental value, of course), 2 Lenovo Windows tablets, a Lenovo Android Tablet, an Nvidia Shield, 2 Thinkpad 230X's (I built those, one of which has 3 terabytes because I was able to swap out the wwan card with a second ssd) a Thinkpad T430 (built that one too), an 11 inch Macbook Air (my baby, I put a one terabyte hard drive in that, too), and, of course, my iconic 13 inch, 2015 Macbook Pro.

I won't bore you with my gizmos. If it has a screen, chances are that I bought the parts separately to put together and either put each device together, or tried and failed, which happens sometimes. I also have four phones and have found merit to both IOS and Android. I still don't know which I like better so I keep flip-flopping between the two.

Many guys go fishing, or play golf, or go bowling. My hobbies are computers and engineering. I also spend far too much time working through cross platform communications. I do this because there are things you can do with Windows that you can't do with Os X, and vise-versa, and, of course, there are things you can do with Linux that you can't do with either Windows or Os X.

I have spent years streamlining the production and completion of legal forms, and had built a method for getting a couple's divorce papers completed (all of them, both Husband and

Wife) in a matter of minutes. That process involves interlinking fields in Adobe and I had to learn a little Javascript and HTML to make it all work.

I don't have a formal computer degree, but as a child of the 80's growing up with an Apple IIe (my first computer), TRS-80 (yes, we called them "Trash-80's), Commodore 64, not to mention the Ataris (2600, 5200, etc) Intellivision, etc, there wasn't a machine I didn't try to get my hands on and found merit (and often beauty) in its engineering. I have built my own websites, I have used almost every word processing program that is in existence (trying to find the best one, of course) and I use Dragon "Naturally Speaking" in both Windows and Os X to turn my speech into text when I am working on pleadings, email, and even texting from my computer.

My quest has always been the same: to find a better, faster, computerized method for completing all of the tasks necessary for the practice of law. People ask me how it is that I have practiced law since 1996 without a secretary or legal assistant and the answer is that it's very doable if you can get your machines to do the work for you, which I have.

If you have questions or need help automating, email me, send me a text, or you can even play it old school with a good old-fashioned phone call.

Jeff Rapkin