New Lawyer Program

KENTUCKY BAR ASSOCIATION

Cybersecurity Training for New Lawyers

On Demand

Presented by:
The Kentucky Bar Association
Continuing Legal Education Commission

Caroline J. Carter, Laura Cole, Cassie H. Cooper, and Lori J. Reed, Editors

Published October 2025

Editor's Note: These *New Lawyer Program* handbook materials are intended to provide current and accurate information about the subject matter covered as of the original publication date. No representation or warranty is made concerning the application of legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of the *New Lawyer Program* disclaim liability therefor. Attorneys using these materials or information otherwise conveyed during the program, in dealing with a specific legal matter, have a duty to research original and current sources of authority. In addition, opinions expressed by the authors and program presenters in these materials do not reflect the opinions of the Kentucky Bar Association, its Board of Governors, Sections, Divisions, Committees, or members.

The Kentucky Bar Association would like to give special thanks to the volunteer authors who contributed to these program materials.

CYBERSECURITY CONCERNS FOR NEW ATTORNEYS

Jeff Sallee[*]

I. CYBERSECURITY CONCERNS FOR NEW ATTORNEYS

A. The Ethical Requirements Relating to Cybersecurity

1. SCR 3.130(1.1) – Competence.

> Maintaining Competence
>
> (6) To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

2. SCR 3.130(1.6) – Confidentiality of information.

> (14) A lawyer must act competently to safeguard information relating to the representation of a client 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 1.1, 5.1 and 5.3.
>
> (15) When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

[*] jeff.sallee@jeffsallee.com.

3. SCR 3.130(5.3) – Responsibilities regarding nonlawyer assistants.

> (2) Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that nonlawyers in the firm will act in a way compatible with the Rules of Professional Conduct. *See* Comment [1] to Rule 5.1. Paragraph (b) applies to lawyers who have supervisory authority over the work of a nonlawyer. Paragraph (c) specifies the circumstances in which a lawyer is responsible for conduct of a nonlawyer that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer.

4. Ethics Opinion KBA E-446 – Cyber Security.

> **Question #1:** Does an attorney have an ethical responsibility to implement cybersecurity measures to protect clients' information?
>
> **Answer:** Yes
>
> **Question #2:** Does an attorney have an ethical responsibility to advise clients about cyberattacks against the law practice and/or breaches of security?
>
> **Answer:** Qualified Yes
>
> **Question #3:** Can an attorney utilize third parties and/or non-lawyers to plan and implement cybersecurity measures?
>
> **Answer:** Yes
>
> **Question #4:** Does an attorney have an ethical responsibility to ensure that law firm employees, as well as third parties employed by, retained by, or associated with the lawyer, comply with the attorney's cybersecurity measures?
>
> **Answer:** Yes

5. Recent ABA Formal Ethics Opinions

   a. Formal Opinion 502 – Communication with a Represented Person by a *Pro Se* Lawyer.

   Some attorneys who represented themselves believed that they could contact other parties directly because they were not representing another party in the matter.

This opinion clarified that attorneys representing themselves in a matter are representing someone: themselves. Correspondingly, the prohibition against contacting represented parties directly still applied.

b. Formal Opinion 503 – "Reply All" in Electronic Communications.

If an attorney (sending lawyer) copies their client on an email to another attorney (receiving lawyer), the receiving lawyer has an implied consent from the sending lawyer to contact the copied clients by replying using "Reply All."

The receiving lawyer does NOT violate Rule 4.2 unless the sending lawyer expressly states there is no implied consent to contact the clients directly.

The better practice is for the sending lawyer to forward the client a separate copy of the email and not include the receiving lawyer on that separate copy.

B. Law firms are frequently breached. Comparitech published an article[1] in 2024 that documented the publicly acknowledged data breaches. The average ransomware demand is about $2.5M and the average amount paid is over $1.6M. In 2023, there were 45 documented ransomware attacks on law firms involving over 1.5M client records.

Several law firms have experienced or settled litigation cyberattacks in the recent past.

1. Orrick, Herrington & Sutcliffe was attacked in Feb 2023. Well over 637,000 client files with names, addresses, DOBs, and SSNs were stolen. They settled in October 2024 for $8M.[2]

2. Hastings, Cohan & Walsh, a real estate law firm, was breached in 2024. The hacker then used a BEC attack and sent a client an email with wiring instructions for the purchase of home. In August 2024, hackers spoofed wire instructions via email compromise. The client wired $726,000 to the fraudster's account. The bank was able to recover $129,000 but the client was out $597,000. The client sued the law firm, and the firm's insurance carrier refused to cover the loss.

[1] Moody, R., "Law firms hit with average ransom demand of $2.5 million," *Comparitech.com*, Aug. 1, 2024, *available at* https://www.comparitech.com/blog/information-security/ransomware-attacks-law-firms.

[2] Naqvee, Z., "ACT FAST Americans have hours left to claim $10,000 checks from $8m data breach settlement and all you need is a receipt," *The U.S. Sun.*, *available at* https://www.the-sun.com/money/12761982/americans-claim-data-breach-settlement/.

3. Bryan Cave Leighton Paisner represented Mondelez, a snack food company in 2023. The law firm was breached and more than 51,000 current and former Mondelez employees had their PII compromised.[3] The law firm and their client agreed to a $750,000 settlement with the proposed class action lawsuit. The plaintiffs' law firm will likely receive an additional $250,000 in fees from the two.

C. Cost to recover from a data breach: These numbers come from the annual Varonis data breach report's 2024 update. *See* the article for links to their sources.[4]

1. The average total cost of a ransomware breach is $4.88M (IBM).

2. In more than 70 percent of cases, breaches can be traced back to organized crime groups (Verizon).

3. Forty-nine percent of costs are incurred more than a year after a data breach (IBM).

4. On average, a data breach is discovered 194 days after day 0.

5. The average time to contain a breach was 64 days in 2024, nine days less than in 2023 (IBM).

D. This session will cover several critical things to have in place for cybersecurity.

1. Passwords.

a. Use strong passwords.

b. Do not reuse passwords.

c. Change your passwords regularly.

2. Use multi-factor authentication wherever possible.

3. Secure your wireless network.

4. Have a cybersecurity program.

a. Create and enforce policies.

[3] Thomas, D., "Mondelez, law firm Bryan Cave reach deal to end data breach class action," *Reuters*, Oct. 4, 2024, *available at* https://www.reuters.com/legal/litigation/mondelez-law-firm-bryan-cave-reach-deal-end-data-breach-class-action-2024-10-04/.

[4] Sobers, R., "82 Must-Know Data Breach Statistics [updated 2024]," Varonis, Nov. 15, 2024, *available at* https://www.varonis.com/blog/data-breach-statistics.

b. Train users.

c. Understand social engineering.

5. Patch and replace your systems on a regular basis. If your system no longer receives security updates, you need to replace it.

6. Backup your data and verify that you can restore your data in an emergency.

7. Have a security expert review your systems and websites.

II. PHISHING TRAINING – A BRIEF HISTORY OF PHISHING AND HOW TO SPOT A PHISHING EMAIL

Social engineering is the general term that refers to the use of deception to convince targeted people into providing non-public information of a personal nature. This information is then used for fraudulent purposes.

A. What are the major kinds of social engineering?

1. Phishing.

This is the use of email as the method of obtaining information. Phishing campaigns are generally sent indiscriminately to thousands or even millions of email addresses.

a. Spear phishing differs from general phishing by the targets. Spear phishing targets fewer people with emails that were specifically designed to be of interest to the recipients.

b. Whale phishing is similar to spear phishing, but the targets are limited to highly important individuals, such as senior corporate executives, extremely wealthy individuals, politicians, or actors.

2. Other forms of social engineering are becoming more popular.

a. Smishing is like phishing but uses SMS text messages instead of emails. Unlike emails, the recipient cannot hover over links to inspect the destination of links. A popular trend for smishing is for a hacker to send someone money via a cash app then send a follow-up message that it was an accident. The victim is asked for the money to be returned. The funds sent to the victim were from a stolen credit card, which the credit card company will get back from the victim's account. The "refund" is not recoverable because the account is closed, and the criminal is unknown. The victim cannot recover the funds because they intentionally sent the money, and their only recourse is to go after the criminal.

b. Vishing is social engineering using voice communications (phone calls). A phone call is often made as a follow-up to a spear phishing campaign.

c. Business email compromise (BEC) is a special form of social engineering that is much more dangerous than phishing. BEC happens when a hacker has been able to control an individual's email account. The hacker will often lurk and read the emails, waiting for the right moment to act. This often happens when the account holder is unavailable, making it difficult to confirm the details of an email. The hacker then sends a fraudulent email from the email system, asking the recipient to do something seemingly legitimate. Examples are:

  i. The CEO emails a CFO with instructions to wire money to complete a transaction that they had been working on.

  ii. An attorney is provided an account to wire settlement funds.

  iii. A title company receives a request to close a sale early by wiring the funds to a new account because the old account was mistakenly entered on the original paperwork.

d. QR (quick response) code hijacking.

People see these squares of pixels everywhere these days. If you scan the QR code with your smartphone camera, it will allow you to link to a website. Many restaurants provide them at tables for patrons to scan to see the menu. Hackers can place their own QR codes over legitimate QR codes knowing that people usually follow these links without paying attention to the underlying URL or address of the destination. One common trend is for malicious QR codes to be placed over QR codes at parking sites. A person thinks they just paid to park in a lot but instead just paid a criminal.

e. Deepfake videos and calls.

A deepfake is a computer simulation that someone creates with the intent to represent an individual. The likeness is then used to imply that the actual individual is performing the activities. Artificial intelligence has been used to make these deepfakes more interactive and less identifiable as an artificial construct. Criminals have used deepfakes to convince victims to transfer money because they thought the video chat was legitimate.[5]

[5] Edwards, B., "Deepfake scammer walks off with $25 million in first-of-its-kind AI heist," ARS Technicia, Feb. 5, 2024, *available at* https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/.

B. Phishing Training

The CLE session will include examples of phishing campaigns and how to identify warning signs that an email could be a phishing attempt.

1. In general, email can be divided into malicious email, legitimate email, and graymail.

    a. Over half of all emails sent today are malicious. This is email that contains viruses of malicious links.

    b. About a third of email is graymail. This is an email that is likely to be unwanted by the recipient, but not necessarily malicious in nature. This is what we generally call spam.

    c. Legitimate email is the remaining 15 percent. This is an email that you wanted to receive and was sent by someone you know or was otherwise expected.

2. “Red flags” is a term used in phishing training to suggest aspects of an email that should make you very suspicious that the email is a phishing attempt. These include:

    a. Tone is threatening, urgent, or causes an emotional response.

    b. Requests for personal information that they should already have.

    c. The subject line is irrelevant or doesn’t match the message content.

    d. Request for your password, login credentials, or to click a link.

    e. Contains attachments with executable extensions such as .exe.

    f. Request to perform an urgent financial transaction out of the norm.

3. If you think the email might be a phishing email, you should take the following actions:

    a. If suspicious, call the sender using a known phone number. Do not rely on the information you see in the email.

    b. Hover over the links to see if the link sends you where it should. If it takes you somewhere odd, do not click on the link. The Law Practice Committee published an article “Phishing and Ransomware” in the November 2021 edition of the *Bench & Bar* that addressed some of the issues with email addresses and suspicious domains.

    c. Block the sender as sending junk mail.

d. Do NOT open the email. Use preview mode.

e. Do NOT click on the links.

f. Do NOT open suspicious attachments, especially ones that end in .exe.

g. Consider if you want to reply. Replying to spam will let them know this is an active email account.

C. Three Hacking Methods Related to Passwords

If hackers know two of three items from usernames, passwords, and the service being used, they have a method to find the unknown third component.

1. Brute force.

With brute force, the hacker knows the username and the service being used. For example, the hacker could know that I use the username "jeff.sallee" at the service myorg.com.

a. Offline hacking.

If the hacker can obtain a copy of the hashed (somewhat encrypted) password table from myorg.com, then the hacker can set up one or more computers to systemically guess my password until the system cracks the password or the hacker decides to give up. The length and complexity of the password will determine how long it takes to crack a password. For an eight-character password the time is less than one second, even if the password uses a mix of upper- and lowercase letters, numbers, and special characters.

b. Online hacking.

If the target system does not have security measures in place to lock out unsuccessful password attempts or some form of security warning in place to warn that this could be happening, a hacker can start guessing passwords right away and keep doing so until access is granted, the hacker gives up, or so someone in IT notices the activity and takes measures to stop the attempts.

2. Credential stuffing.

With credential stuffing, the hacker knows the username and the password being used. For example, the hacker could know that I used the username "jeff.sallee" and the password "PassW0rd1" at some point. This information is readily available for purchase on the dark web from past hacks. You can see if your account is on one of these databases by looking at https://haveibeenpwned.com/. You will not be informed of the password that was compromised, but you will see the company involved in the known data breach, the year of the breach, and the kinds of information believed to be involved in the breach.

a. The software to automate the credential stuffing can be downloaded at no cost.

b. A configuration file to target a site using the known credentials can be downloaded for a nominal fee.

c. The hacker can rent or purchase proxies to hide the true source of the attack for a nominal fee.

d. The cost of the credentials will depend on several factors: how recently the hacked credentials were obtained; the kind of system the credentials were stolen from; how famous the target is, etc. The average cost for online banking credentials was $35 in 2020.

e. The cost to run the software, find the credentials, and access the accounts is $0.

The net cost for trying to use 100 online banking credentials on a few dozen other financial systems could be less than $4,000. Anyone who uses the same username and password on these sites that they used on the site that was hacked now has the new site compromised. The new targets may not even realize the account was not accessed by the true owner because the hacker only hit the users' account once and the correct password was used.

3. Password spraying.

With password spraying, the hacker knows the password and service being used. For example, the hacker could know all of the usernames for acb123.org. The hacker then uses a commonly used password, such as "password" or "12345678" for all those accounts. Just like the credential spraying attack, each individual attack was for one username and one password. These common passwords are often rejected by some systems for just this reason.

D. Videos Related to Phishing and Social Engineering

1. Social media files available to the general public for phishing awareness:

a. Phishing email awareness training from Simplilearn – https://www.youtube.com/watch?v=XBkzBrXlle0&t=46s

b. Free course from IBM Technology – https://www.youtube.com/watch?v=gWGhUdHItto

c. Demonstration of social media's impact on your security – https://www.youtube.com/watch?v=F7pYHN9iC9I

2. Some sites that are interesting for attorneys to review:

   a. TechLaw Crossroads – https://www.techlawcrossroads.com/. Exploring the intersection of technology and the law by Steve Embry.

   b. Cybersecurity & Infrastructure Security Agency – https://www.cisa.gov/. A great site for cybersecurity education. Some free services are available.

   c. Justia Blawgsearch – https://blawgsearch.justia.com/topblogs?popmode=all. A great place to go if you want to find a law blog for your practice area.