

Ethical Obligations of Title Agents and Attorneys for Cyber Security

Brad Jones
Vice President | Claims Counsel
Mississippi Valley Title
Old Republic National Title Insurance Company
1022 Highland Colony Parkway, Suite 200
Ridgeland, MS 39157
P.O. Box 2901 | Madison, MS 39130-2901
bjones@mvt.com



Ethical Obligations of Title Agents and Attorneys for Cyber Security

If you are not concerned about cyber security, you don't know enough about it.

Brad Jones
Vice President | Claims Counsel

Agenda

1. Ethical Obligations
2. Common Cyber Threats
3. Protecting Against Cyber Threats
4. Victim Response
5. Insurance Coverage

Competence

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.

Technology Amendment to Comment [8] to ABA Model Rule 1.1 Competence

“It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.”

Arizona Bar Opinion 09-04 (December, 2009).

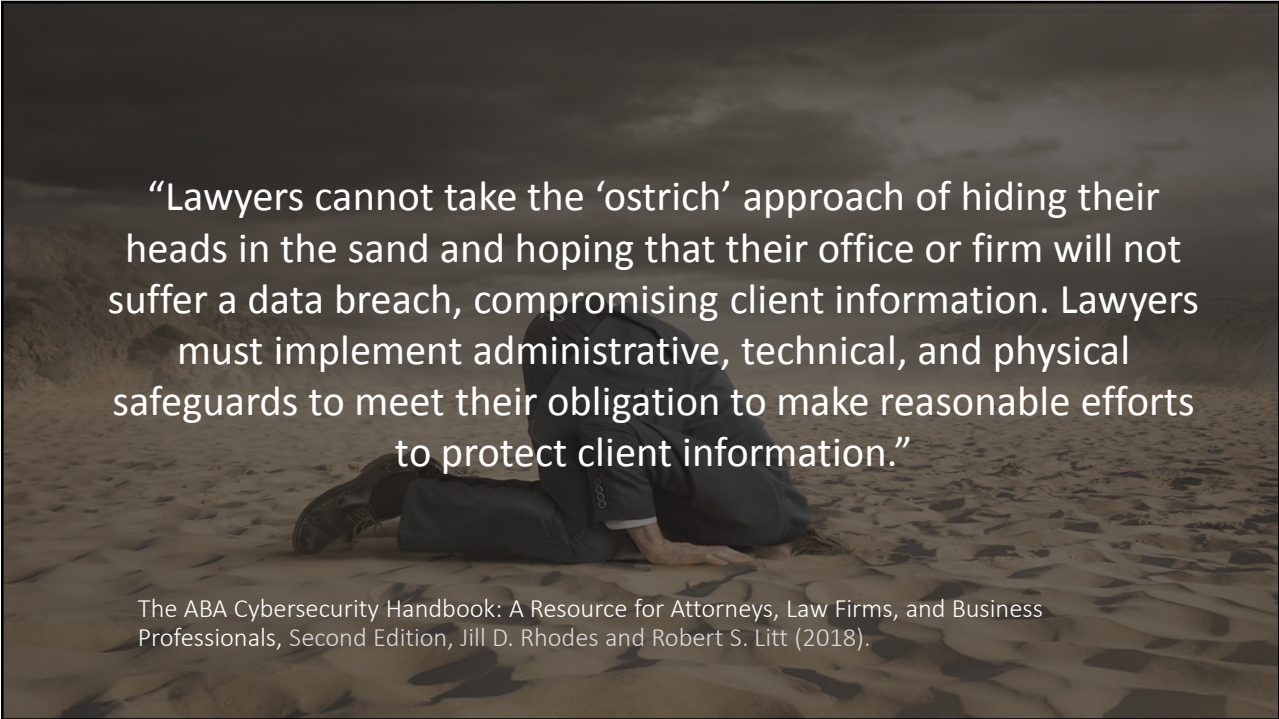
Confidentiality of Information

“A lawyer shall make reasonable efforts to prevent the inadvertent, or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

2012 Amendment to ABA Model Rule 1.6(c)

The more sensitive the data being transmitted and the lower the legal or technological protection afforded by the method of communication, the more likely it is that special precautions may be reasonably necessary to protect client confidences.

Comment [17] to ABA Model Rule 1.6(c)



“Lawyers cannot take the ‘ostrich’ approach of hiding their heads in the sand and hoping that their office or firm will not suffer a data breach, compromising client information. Lawyers must implement administrative, technical, and physical safeguards to meet their obligation to make reasonable efforts to protect client information.”

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition, Jill D. Rhodes and Robert S. Litt (2018).

Safekeeping Property – Nondelegable Duty

Only a lawyer admitted to practice in this jurisdiction or a person under direct supervision of the lawyer shall be an authorized signatory or shall authorize transfers from a client trust account.

Rule 1.15(f)(1), Alabama Rules of Professional Conduct

A lawyer should hold the property of others with the care required of a professional fiduciary.

Comment to Rule 1.15, Alabama Rules of Professional Conduct

Ethical Guidance

- Formal Ethics Opinion 477R (revised May 22, 2017), ABA Standing Committee on Ethics and Professional Responsibility.
- In re Anderson, 685 S.E.2d 711 (Ga. 2009).
- Tennessee Board of Professional Responsibility Formal Ethics Opinion 2015-F-159 (2015) (“The security precautions that lawyers take need not be infallible; they must be reasonable under the circumstances.”).
- Responsibilities of a Partner or Supervisory Lawyer, Rule 5.1, Alabama Rules of Professional Conduct.
- Responsibilities Regarding Nonlawyer Assistants, Rule 5.3, Alabama Rules of Professional Conduct.

Email Account Compromise Scheme

Resource Real Estate Services, LLC v. Evanston Ins. Co., 2017 WL 6608000 (D. Md. 2017).

Legitimate email address:

john-doe@abc.com

Fraudulent email address:

john_doe@abc.com



Directs the escrow agent to wire the seller's proceeds to the imposter's bank account.

Email Account Compromise Scheme – Numbers

480%
TITLE COMPANIES

2,370%
EXPOSED LOSSES

103
COUNTRIES

Increase in EAC scams reported by title companies to the FBI in 2016.



Increase in exposed losses between January, 2015 and December, 2016.



Fraudulent transfers have been sent to 103 countries.



Email Account Compromise Scheme

\$16,000,000

2016

\$969,000,000

2017

Amount of real estate purchase funds “diverted or attempted to be diverted” from real estate purchase transactions, and wired to “criminally controlled” accounts.

[Here's another cyber scam that could cost you thousands](#), Miami Herald, October 30, 2017 (data provided by FBI).

Errors and Omissions Insurance

Policy Exception

“arising out of any actual or alleged conversion, misappropriation, commingling, defalcation, theft, disappearance, [or] insufficiency in the amount of escrow funds, monies, monetary proceeds, funds or property, or any other assets, securities, negotiable instruments or any other thing of value.”

Resource Real Estate Services, LLC v. Evanston Ins. Co., 2017 WL 660800 (D. Md. 2017).

Phishing and Social Engineering

The Human Problem

Phishing Emails

- Mass emails sent by cyber criminals that seek to obtain sensitive information such as usernames, passwords, bank account details, or credit card details.

Spear Phishing

- Phishing emails sent to specific individuals or companies. Cyber criminals gather personal information about their target to increase their probability of success.

Social Engineering

- Psychological manipulation of people to get them to perform specific acts or divulge confidential information.



Ransomware



OLD REPUBLIC TITLE

Password Security

Length of Password

Password Reuse & Sharing

Keystroke Logging

Brute Force Attack

Data Breach



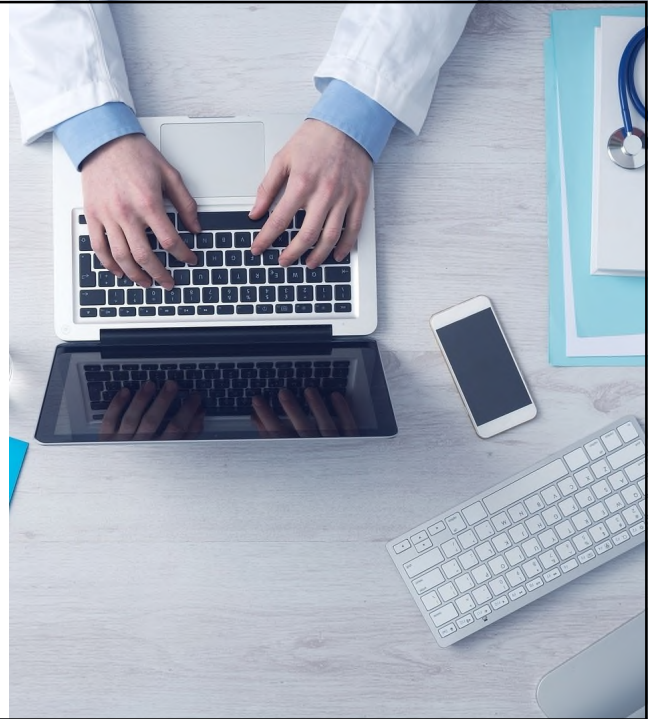
OLD REPUBLIC TITLE

Password Manager

Editor's Choice – PC Magazine

- 1 Dashlane
- 2 Keeper Password Manager
- 3 Sticky Password Premium
- 4 LogMeOnce

The Best Password Managers of 2018, PC Magazine, Neil J. Rubenking, December 7, 2017

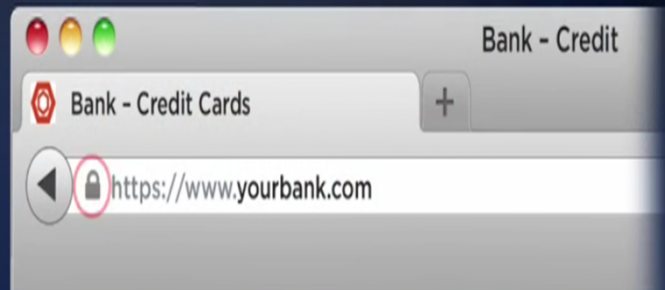


Two-Factor Authentication (2FA)



Internet Security

- Make sure any website that you visit that contains or requests personal information is secure.
 - Look for the **https** in the web address or a padlock icon in your browser window.
 - Consider setting up a Virtual Private Network.
- Enable WPA2 encryption on your wireless router.
- Enable the firewall on your network.
- Avoid using WI-FI hotspots and free wireless charging stations.



Employee Training

The Human Problem

- Responsibilities of a Partner or Supervisory Lawyer
 - Rule 5.1, Alabama Rules of Professional Conduct
- Responsibilities Regarding Nonlawyer Assistants
 - Rule 5.3, Alabama Rules of Professional Conduct
- In re Anderson, 685 S.E.2d 711 (Ga. 2009).

Bank Account and Wire Transfer Security

Choice Escrow and Land Title, LLC v. BancorpSouth Bank, 754 F.3d 611 (8th Cir. 2014).

ATTACKER



Created a wire transfer for \$440,000 to a bank account in the Republic of Cypress.

TROJANS HORSE



Creates email message that includes a link that link, when clicked on, will download a virus to the victim's computer.



CHOICE TITLE AND ESCROW



Choice employee clicks the link and downloads a computer virus that allows the attacker to take control Choice's Computer.

Banking and Wire Transfer Controls



Positive Pay



Dual Controls



ACH Blocks and Filters



Dedicated Computer



Understanding Cyber Insurance

- Broad cyber coverage is not currently available.
- Failure to follow minimum required practices exclusion.
- Exclusions for losses directly or indirectly caused by “the input of Electronic Data by a natural person having authority to enter the Insured’s Computer System.”
- May not cover important losses, such as the cost of a company’s damaged reputation or stolen intellectual property.
- Premiums on cyber policies are expected to soar to \$20 billion in 2025, up from \$3 billion in 2016.



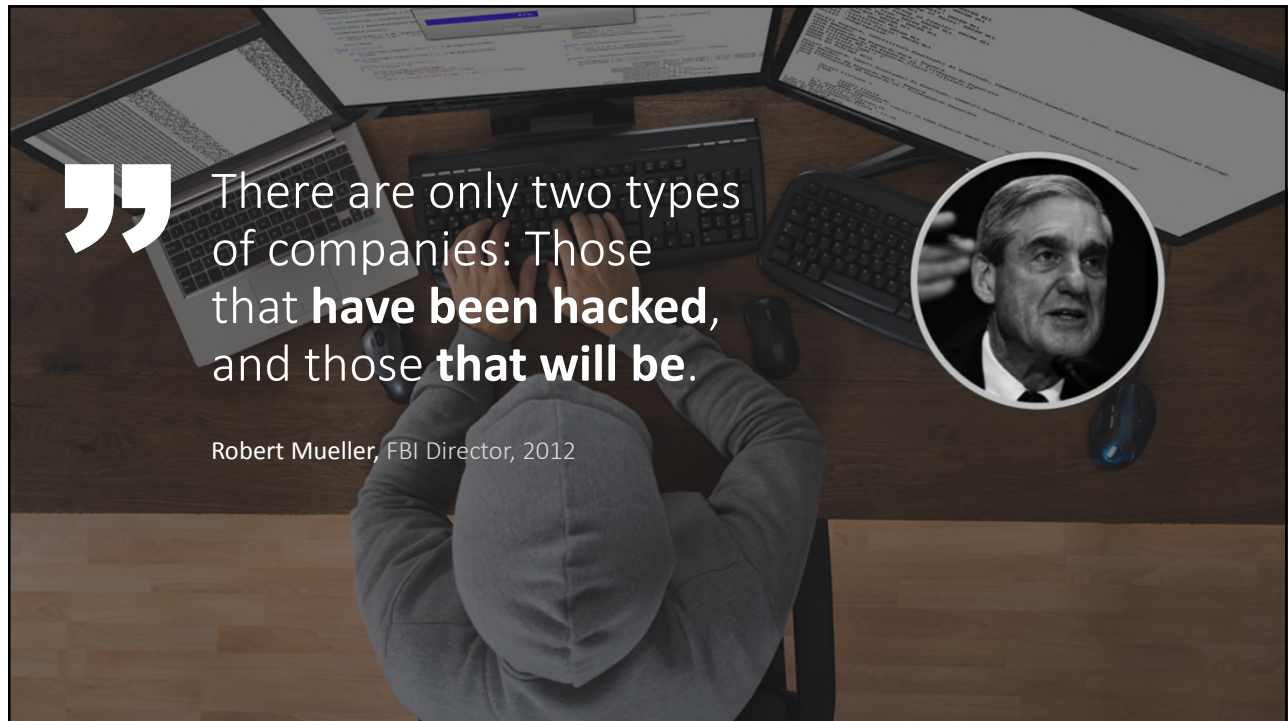
Victim Response to Email Account Compromise Scheme

- 1 Notify your bank and the corresponding bank.
- 2 Notify local FBI office and file a complaint with IC3.
- 3 Consider civil injunction against corresponding bank.
- 4 Refer to FBI PSA on Business Email Compromise Schemes.
- 5 Financial Fraud Kill Chain for international wire transfers.

Summary

Security Checklist

- Avoid clicking links or downloading attachments in untrustworthy offers and emails.
- ✓ Train your employees in cyber security principles.
- Install current antivirus, firewall, spam filtering, anti-phishing, and anti-spyware software.
- Keep offline backup copies of important business data and information.
- ✓ Turn your computer off at night.
- Avoid sending sensitive information accessing banking websites over unsecured WIFI connections.
- Confirm wiring instructions by phone (using phone number obtained from an independently verified source).
- Enable two-factor authentication on email and bank accounts.




” There are only two types of companies: Those that **have been hacked**, and those **that will be**.

Robert Mueller, FBI Director, 2012

QUESTIONS  ANSWERS

Brad Jones
Vice President – Claims Counsel

 1022 Highland Colony Parkway, Suite 200
Ridgeland, MS 39157

 Tel. 601.961.4866

 bjones@mvt.com



Reduce Your Risk of Cyberfraud by Practicing **Good Cyber Hygiene**

- Do not click on suspicious emails, attachments or links.
- Keep your operating system up-to-date on all devices.
- Install antivirus software on all devices and keep it up-to-date.
- Keep your firewall turned ON.
- Turn off, lock, or set to “time-out” when your computer/device is not in use.
- Use strong passwords and change them every 90 days.
- Do not use personal information for passwords; rather, include one upper/lower case letter; one special character; one number, etc.
- Use individual employee accounts, not shared email accounts.
- Be careful what you download.
- Avoid websites you don’t trust.
- Do not send wire instructions or other business-sensitive data to/from a personal email account.
- Encrypt all emails containing wire instructions or other business-sensitive data.
- Use only secured email accounts; avoid using free, web-based email accounts for business communications.
- Be aware that the email accounts of other parties to a transaction may be unsecured or easily hacked.



Brad Jones
Vice President - Claims Counsel
bjones@mvt.com
T: 601.961.4866



Top 10 Tips To Avoid Cybercrime Losses

- 1** Create a log of all approved parties' phone numbers at the start of a transaction.
- 2** Avoid using free, web-based email accounts for business communications.
- 3** Prior to closing, execute an agreement with the seller/borrower indicating the method of funds transfer: check or wire.
- 4** Remember: transactions that result in a large cash payment to a refinance borrower or seller are highly susceptible to attack.
- 5** Question and confirm by phone with approved parties any deviation to the funding agreement (see 1); changes are not common and may indicate fraud.
- 6** Confirm wiring instructions by phone with approved parties (see 1) prior to sending.
- 7** Confirm receipt of wired funds by phone with the intended recipient (see 1).
- 8** Practice good cyber hygiene: keep antivirus software up-to-date, don't click suspicious links, and use strong passwords.
- 9** Slow down and stay in control; a slow, confirmed closing is still acceptable.
- 10** If you suspect fraud, act immediately; contact your bank and appropriate authorities.



Brad Jones
Vice President - Claims Counsel
bjones@mvt.com
T: 601.961.4866





OLD REPUBLIC TITLE

BEWARE OF WIRE FRAUD

Since 2013, there have been 40,000 incidents worldwide involving losses of over **\$5.3 BILLION.** - FBI, BEC, EAC (2016)



It is estimated there are **4,000 HACK ATTEMPTS** per day nationwide. - FBI

FRAUDULENT WIRING instructions are being sent to real estate agents, title companies and customers

HOW TO PROTECT YOURSELF

-  **BE WARY** of free, web-based email accounts; they are easily hacked.
-  **ALWAYS VERIFY** changes in payment instructions and confirm requests for transfer of funds.
-  **CAREFULLY EVALUATE** any requests for secrecy or pressure to take action quickly.
-  **CALL, DON'T EMAIL:** Confirm all wiring instructions by phone before transferring funds. Use the phone number from the title company's website or a business card.
-  **BE SUSPICIOUS:** It's not common for title companies to change wiring instructions and payment info.
-  **CONFIRM IT ALL:** Ask your bank to confirm not just the account number but also the name on the account before sending a wire.
-  **VERIFY IMMEDIATELY:** You should call the title company or real estate agent to validate that the funds were received. Detecting that you sent the money to the wrong account within 24 hours gives you the best chance of recovering your money.
-  **FORWARD, DON'T REPLY:** When responding to an email, hit forward instead of reply and then start typing in the person's email address. Criminals use email address that are very similar to the real one for a company. By typing in email addresses you will make it easier to discover if a fraudster is after you.

IF YOU THINK YOU MIGHT BE A VICTIM:

1



Using a previously known phone number, call the supposed sender of the email to authenticate the change request - don't call the number on the email.

2



If you suspect fraud, immediately notify the financial institutions and escrow agent involved in the transaction.

3



Contact your local law enforcement authorities, and file a complaint with the FBI's Internet Crime Complaint Center.

Brad Jones
Vice President - Claims Counsel
bjones@mvt.com
Phone: (601) 961-4866

Effective 9.6.17 LE | Old Republic Title is providing this information as a free customer service and makes no warranties or representations as to its accuracy.

Old Republic Title strongly recommends that consumers confer with their title insurer as underwriting requirements vary among companies and further, obtain guidance and advice from qualified professionals, including attorneys specializing in Real Property, Trusts and/or Title Insurance to get more detailed, and current, information as to any particular situation affecting them.

Source : ALTA



OLD REPUBLIC INSURANCE GROUP



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE E-MAIL ACCOUNT COMPROMISE THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION

Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type¹ in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

BACKGROUND

The victims of the BEC/EAC scam range from small businesses to large corporations. The victims continue to deal in a wide variety of goods and services, indicating that no specific sector is targeted more than another.

It is largely unknown how victims are selected; however, the subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails requesting additional details regarding the business or individual being targeted (name, travel dates, etc.).

Some individuals reported being a victim of various Scareware or Ransomware cyber intrusions immediately preceding a BEC incident. These intrusions can initially be facilitated through a phishing scam in which a victim receives an e-mail from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the subject(s) unfettered access to the victim's data, including passwords or financial account information.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams. The victims of these scams are usually U.S. based and may be recruited as unwitting money mules². The mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds to another bank account, usually outside the U.S., upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme.

STATISTICAL DATA

The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses³. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries.

Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom have also been identified as prominent destinations.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and December 2016**:

Domestic and international incidents:	40,203
Domestic and international exposed dollar loss:	\$5,302,890,448

The following BEC/EAC statistics were reported in victim complaints to the IC3 from **October 2013 to December 2016**:

Total U.S. victims:	22,292
Total U.S. exposed dollar loss:	\$1,594,503,669

Total non-U.S. victims:	2,053
Total non-U.S. exposed dollar loss:	\$626,915,475

The following BEC/EAC statistics were reported by victims via the financial transaction component of the new IC3 complaint form, which BECame available in June 2016⁴. The following statistics were reported in victim complaints to the IC3 from **June 2016 to December 2016**:

Total U.S. financial recipients:	3,044
Total U.S. financial recipient exposed dollar loss:	\$346,160,957

Total non-U.S. financial recipients:	774
Total non-U.S. financial recipient exposed dollar loss:	\$448,464,415

SCENARIOS OF BEC/EAC

Based on IC3 complaints and other complaint data, there are five main scenarios by which this scam is perpetrated.

Scenario 1: Business Working with a Foreign Supplier

A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears similar to a legitimate request. Likewise, requests made via facsimile or telephone call will closely mimic a legitimate request. This particular scenario has also been referred to as the "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme."

Scenario 2: Business Executive Receiving or Initiating a Request for a Wire Transfer

The e-mail accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular scenario has been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail

An employee of a business has his or her personal e-mail hacked. This

personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not BECome aware of the fraudulent requests until that business is contacted by a vendor to follow up on the status of an invoice payment.

Scenario 4: Business Executive and Attorney Impersonation

Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

Scenario 5: Data Theft

Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipients of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario even if they were able to successfully identify and avoid the traditional BEC scam. This data theft scenario of the BEC scam first appeared just prior to the 2016 tax season.

TRENDS

W-2/PII Data Theft

This scenario of BEC/EAC was identified in 2016 in which a human resource department or counterpart was targeted with a spoofed e-mail seemingly on behalf of a business executive requesting all employee PII or W-2 forms for tax or audit purposes. The request appeared to coincide with the 2016 U.S. tax season, which runs from January through April. The number of complaints and reported losses peaked in April 2016, although complaints were still submitted by victims throughout 2016. Victims appeared to be both the businesses responsible for maintaining PII data and the employees whose PII was compromised. In several instances, thousands of employees were compromised. Employees filed identity theft-related complaints with IC3 that included reported incidents of fraudulent tax return filings, credit card applications, and loan applications.

Resurgence of Original Scheme

The IC3 saw a 50% increase in the number of complaints in 2016 filed by businesses working with dedicated international suppliers. This scenario was described in the earliest BEC/EAC complaints and quickly evolved into more sophisticated scenarios. In some instances, instead of requesting a change in a single remittance or invoice payment, BEC/EAC perpetrators changed the remittance location to redirect all incoming invoice payments. The fraudulent request appeared to be facilitated through a spoofed e-mail or domain.

Real Estate Transactions

The BEC/EAC scam targets all participants in real estate transactions, including buyers, sellers, agents, and lawyers. The IC3 saw a 480% increase in the number of complaints in 2016 filed by title companies that were the primary target of the BEC/EAC scam. The BEC/EAC perpetrators were able to monitor the real estate proceeding and time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one account to a different account under their control.

SUGGESTIONS FOR PROTECTION

Businesses with an increased awareness and understanding of the BEC/EAC scam are more likely to recognize when they have been targeted by BEC/EAC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially for front line employees who may be the recipients of initial phishing attempts) have proven highly successful in recognizing and deflecting BEC/EAC attempts.

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time to verify the legitimacy of the request.

The following list includes self-protection strategies:

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what you post to social media and company websites, especially job duties and descriptions, hierarchal information, and out-of-office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a two-step verification process. For example:
 - Out-of-Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this two-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
 - Digital Signatures: Both entities on EACH side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
- Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
- Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.
- Consider implementing two-factor authentication for corporate e-mail accounts. Two-factor authentication mitigates the threat of a subject gaining access to an employee's e-mail account through a compromised password by requiring two pieces of information to log in: (1) something you know (a password) and (2) something you have (such as a dynamic PIN or code).
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, a detection system for legitimate e-mail of abc_company.com would flag fraudulent e-mail from abc-company.com.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

A complete list of self-protection strategies is available on the United States Department of Justice website www.justice.gov in the publication titled "[Best Practices for Victim Response and Reporting of Cyber Incidents](#)."

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer.
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of

Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.

- File a complaint, regardless of dollar loss, with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov

When contacting law enforcement or filing a complaint with IC3, it is important to identify your incident as "BEC/EAC"; also consider providing the following information:

- Originating business name
- Originating financial institution name and address
- Originating account number
- Beneficiary name
- Beneficiary financial institution name and address
- Beneficiary account number
- Correspondent bank if known or applicable
- Dates and amounts transferred
- IP and/or e-mail address of fraudulent e-mail

Detailed descriptions of BEC/EAC incidents should include but not be limited to the following when contacting law enforcement:

- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact, including frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity

1. The IC3 uses descriptions of crime types for categorization purposes. [↔](#)

2. Money mules are defined as persons who transfer money illegally on behalf of others. [↔](#)

3. Exposed dollar loss includes actual and attempted loss in United States dollars. [↔](#)

4. "Financial Recipient" is defined as an account holder who receives the fraudulent funds. [↔](#)

OUCH!

IN THIS ISSUE...

- Overview
- How Password Managers Work
- Choosing Password Managers

Password Managers

Overview

One of the most important steps you can take to protect yourself online is to use a unique, strong password for every one of your accounts and apps. Unfortunately, it is most likely impossible for you to remember all your different passwords for all your different accounts. This is why so many people reuse the same password. Unfortunately, reusing the same password for different

accounts is dangerous, because once someone compromises your password, they can access all your accounts that use the same password. A simple solution is to use a password manager, sometimes called a password vault. These are programs that securely store all your passwords, making it easy to have a different password for each account. Password managers make this simple, because instead of having to remember all your passwords, you only have to remember the master password to your password manager.

How Password Managers Work

Password managers work by storing all your passwords in a database, which is sometimes called a vault. The password manager encrypts the vault's contents and protects it with a master password that only you know. When you need to retrieve your passwords, such as to log in to your online bank or email, you simply type your master password into your password manager to unlock the vault. In many cases, the password manager will automatically retrieve your password and securely log in for you. This makes it simple to have hundreds of unique, strong passwords, since you do not have to remember them.

Some password managers store your vault on your computer or mobile device, while others store it in the Cloud. In addition, most password managers include the ability to automatically synchronize your password vault's contents across multiple devices that you authorize. This way, when you update a password on your laptop, those changes are

Guest Editor

Chris Christianson is an Information Security Consultant based in California, with 20 years of experience and numerous technical certifications. He has spoken at a variety of conferences and is a contributor to many industry articles. Chris can be reached at [@cchristianson](https://twitter.com/cchristianson) and <https://ismellpackets.com>.

Password Managers

synchronized to all your other devices. Regardless where the database is stored, you need to install the password manager application on your system or device to use it.

When you first set up a password manager, you need to manually enter or import your logins and passwords. Afterwards, the password manager can detect when you're attempting to register for a new online account or update the password for an existing account, automatically updating the vault accordingly. This is possible because most password managers work hand-in-hand with your web browser. This integration also allows them to automatically log you into websites.

It's critical that the master password you use to protect the password manager's contents is strong and very difficult for others to guess. In fact, we recommend you make your master password a passphrase, one of the strongest types of passwords possible. If your password manager supports two-step verification, use that for your master password. Finally, be sure you remember your master password. If you forget it, you will not be able to access any of your other passwords.

Choosing a Password Manager

There are many password managers to choose from. In the Resources section, we provide a link to reviews of password managers. Meanwhile, when trying to find the one that's best for you, keep the following in mind:

- Your password manager should be simple for you to use. If you find the solution too complex to understand, find a different one that better fits your style and expertise.
- The password manager should work on all devices you need to use passwords on. It should also be easy to keep your passwords synchronized across all your devices.
- Use only well-known and trusted password managers. Be wary of products that have not been around for a long time or have little or no community feedback. Cyber criminals can create fake password managers to steal your information. Also, be very suspicious of any vendors that developed their own encryption solution.



Password managers are a simple way to securely store and use all your different passwords.

Password Managers

- Avoid any password manager that claims to be able to recover your master password for you. This means they know your master password, which exposes you to too much risk.
- Make sure whatever solution you choose, the vendor continues to actively update and patch the password manager, and be sure you are always using the latest version.
- The password manager should include the ability to automatically generate strong passwords for you and show you the strength of the passwords you've chosen.
- The password manager should give you the option of storing other sensitive data, such as the answers to your secret security questions, credit cards, or frequent flier numbers.

Password managers are a great way to securely store all your passwords and other sensitive data. However, since they safeguard such important information, make sure you use a unique, strong master password that is not only hard for an attacker to guess, but easy for you to remember.

Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at <https://securingthehuman.sans.org/ouch>.

Resources

Top Password Managers of 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS Security Tip of the Day:	https://www.sans.org/tip-of-the-day

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus

OUCH!

IN THIS ISSUE...

- Background
- Passphrases
- Using Passphrases Securely
- Resources

Passphrases

Background

Passwords are something you use almost every day, from accessing your email or banking online to purchasing goods or accessing your smartphone. However, passwords are also one of your weakest points; if someone learns or guesses your password they can access your accounts as you, allowing them to transfer your money, read your emails, or steal your identity. That is why strong passwords are essential to protecting yourself. However, passwords have typically been confusing, hard to remember, and difficult to type. In this newsletter, you will learn how to create strong passwords, called passphrases, that are easy for you to remember and simple to type.

Guest Editor

My-Ngoc Nguyen (pronounced Me-Nop Wynn) is a Certified SANS instructor and CEO/Principal Consultant for Secured IT Solutions. She brings expertise with top certifications and 14+ years of developing, maturing, and managing cyber security programs for various industries and sectors. Follow her on Twitter [@MenopN](#) and on LinkedIn at My-Ngoc "Menop" Nguyen.

Passphrases

The challenge we all face is that cyber attackers have developed sophisticated and effective methods to brute force (automated guessing) passwords. This means bad guys can compromise your passwords if they are weak or easy to guess. An important step to protecting yourself is to use strong passwords. Typically, this is done by creating complex passwords; however, these can be hard to remember, confusing, and difficult to type. Instead, we recommend you use passphrases--a series of random words or a sentence. The more characters your passphrase has, the stronger it is. The advantage is these are much easier to remember and type, but still hard for cyber attackers to hack. Here are two different examples:

Sustain-Easily-Imprison

Time for tea at 1:23

What makes these passphrases so strong is not only are they long, but they use capital letters and symbols. (Remember, spaces and punctuation are symbols.) At the same time, these passphrases are also easy to remember and type.

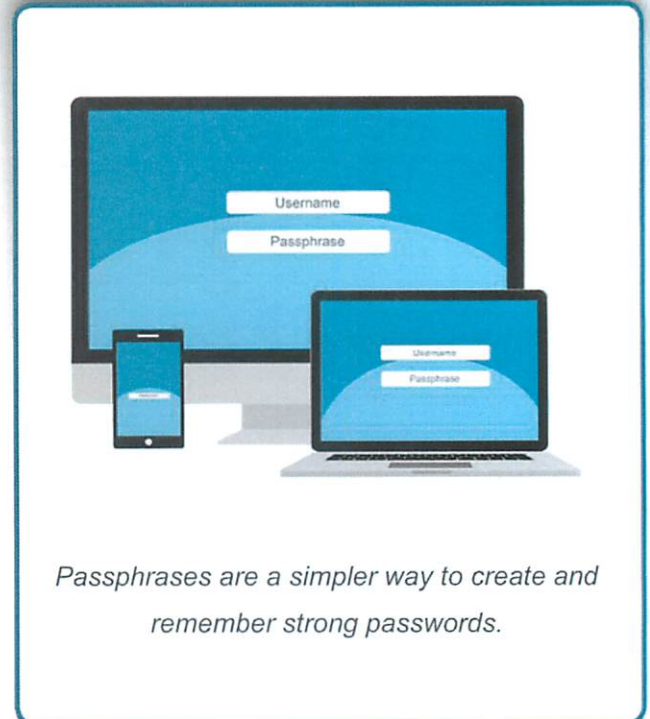
Passphrases

You can make your passphrase even stronger if you want to by replacing letters with numbers or symbols, such as replacing the letter 'a' with the '@' symbol or the letter 'o' with the number zero. If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

Using Passphrases Securely

You must also be careful how you use passphrases. Using a passphrase won't help if bad guys can easily steal or copy it.

1. Use a different passphrase for every account or device you have. For example, never use the same passphrase for your work or bank account that you use for your personal accounts, such as Facebook, YouTube, or Twitter. This way, if one of your accounts is hacked, your other accounts are still safe. If you have too many passphrases to remember (which is very common), consider using a password manager. This is a special program that securely stores all your passphrases for you. That way, the only passphrases you need to remember are the ones to your computer or device and the password manager program.
2. Never share a passphrase or your strategy for creating them with anyone else, including coworkers or your supervisor. Remember, a passphrase is a secret; if anyone else knows your passphrase it is no longer secure. If you accidentally share a passphrase with someone else, or believe your passphrase may have been compromised or stolen, change it immediately. The only exception is if you want to share your key personal passphrases with a highly trusted family member in case of an emergency. One approach is to write down your key personal passphrases (make sure they are not work related), store them in a secure location, and share that location with a highly trusted family member. That way, if something happens to you and you need help, your loved ones can access your critical accounts.
3. Do not use public computers, such as those at hotels or Internet cafes, to log in to your accounts. Since anyone can use these computers, they may be infected and capture all your keystrokes. Only log in to your accounts on trusted computers or mobile devices.



Passphrases are a simpler way to create and remember strong passwords.

Passphrases

4. Be careful of websites that require you to answer personal questions. These questions are used if you forget your passphrase and need to reset it. The problem is the answers to these questions can often be found on the Internet, or even on your Facebook page. Make sure that if you answer personal questions you use only information that is not publicly available or fictitious information you have made up. Can't remember all those answers to your security questions? Select a theme like a movie character and base your answers on that character. Another option is, once again, to use a password manager. Most of them also allow you to securely store this additional information.
5. Many online accounts offer something called two-factor authentication, also known as two-step verification. This is where you need more than just your passphrase to log in, such as a passcode sent to your smartphone. This option is much more secure than just a passphrase by itself. Whenever possible, always enable and use these stronger methods of authentication.
6. Mobile devices often require a PIN to protect access to them. Remember that a PIN is nothing more than another password. The longer your PIN is, the more secure it is. Many mobile devices allow you to change your PIN number to an actual passphrase or use a biometric, such as your fingerprint.
7. If you are no longer using an account, be sure to close, delete, or disable it.

Subscribe to OUCH!

Receive OUCH! monthly in your email inbox. Join the community and subscribe to the OUCH! security awareness newsletter at <https://securingthehuman.sans.org/ouch>.

Resources

- Password Manager: <https://securingthehuman.sans.org/ouch/2015#october2015>
- Two Step Verification: <https://securingthehuman.sans.org/ouch/2015#september2015>
- Lock Down Your Login: <https://lockdownyourlogin.com>
- SANS SEC301 - Five day course on cyber security basics: <https://sans.org/sec301>

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus

OUCH!

IN THIS ISSUE...

- Auto Complete
- Replying to Email
- Distribution Lists
- Emotion
- Privacy

Email Do's and Don'ts

Overview

Email is still one of the primary ways we communicate, both in our personal and professional lives. However, we can quite often be our own worst enemy when using email. In this newsletter, we will explain the most common mistakes people make with email and how you can avoid them in your day-to-day lives.

Guest Editor

Robert M. Lee is the CEO and Founder of Dragos. He is also a SANS Institute Certified Instructor and course author of the FOR578: Cyber Threat Intelligence and ICS515: ICS/SCADA Active Defense and Incident Response courses. He may be found on Twitter [@RobertMLee](https://twitter.com/RobertMLee).

Auto Complete

Auto complete is a common feature found in most email clients. As you type the name of the person you want to email, your email software automatically selects their email address for you. This way, you do not have to remember the email address of all your contacts, just their names. The problem with auto complete is that when you have multiple contacts that share similar names, it is very easy for auto complete to select the wrong email address for you. For example, you may intend to send an email with all of your organization's financial information to "Fred Smith," your coworker in accounting. Instead, auto complete selects the email address for "Fred Johnson," your neighbor. As a result, you end up sending sensitive information to unauthorized people. To protect yourself against this, always double-check the name and the email address before you hit send.

Replying to Email

Most email clients have two options besides 'To' for selecting recipients: 'Cc' and 'Bcc.' Cc stands for "Carbon copy," which means you want to keep people copied and informed. Bcc means "Blind carbon copy," which is similar to Cc; however, no one can see the people you have Bcc'd. Both of these options can get you in trouble. When someone sends you an email and has Cc'd people on the email, you have to decide if you want to reply to just the sender or to everyone that was included on the Cc. If your reply is sensitive, you most likely want to reply only to the sender. If

Email Do's and Don'ts

that is the case, be sure you do not use the 'Reply All' option, which includes everyone. With a Bcc you have a different problem. When you send a sensitive email you may want to privately copy someone using Bcc, such as your boss. However, if your boss then responds to your email using Reply All, all of the recipients will know that you secretly copied your boss on your original email. Whenever someone Bcc's you on an email, do not Reply All, only reply to the person who sent the email.

Distribution Lists

Distribution lists are a collection of email addresses represented by a single name, sometimes called a maillist or a group name. For example, you may have a distribution list with the email address group@example.com. When you send an email to that address, the message gets sent to everyone in the group, perhaps hundreds or even thousands of people. Be very careful what you send to such a list because so many people may receive that message. In addition, be very careful when replying to someone's email on a distribution list. You may intend your reply to be sent to just the individual sender, but the list may automatically include everyone, meaning hundreds (if not thousands) of people are now reading your private email. What can also be dangerous is when auto complete selects a distribution list. Your intent may be to email only a single person, such as your coworker Carl at carl@example.com, but auto complete might accidentally send it to the distribution list you subscribed to about cars at cars@example.com instead.

Emotion

Never send an email when you are emotionally charged. If you are in an emotional state, that email could cause you harm in the future, perhaps even costing you a friendship or a job. Instead, take a moment and calmly organize your thoughts. If you have to vent your frustration, open Microsoft Word or a text editor and type exactly what you feel like saying. Then get up and walk away from your computer, perhaps make yourself a cup of tea or go for a walk. When you come back, delete the message and start over again. Or better yet, pick up the phone and simply talk to the



You can be your own worst enemy when it comes to email. Slow down and double-check what you are sending and to whom before hitting the send button.

Email Do's and Don'ts

person, or speak face to face if possible. It can be difficult for people to determine your tone and intent with just an email, so your message may sound better on the phone or in person.

Privacy

Finally, remember that traditional email has few privacy protections; your email can be read by anyone who gains access to it. Think of email as being similar to a postcard. In addition, once you send an email you no longer have control over it; you can never take it back. Your email can easily be forwarded to others, posted on public forums, released due to a court order, or distributed after a server was hacked. If you have something truly private to communicate, pick up the phone. It is also important to remember that in many countries, email can be used as evidence in a court of law. Finally, if you are using your work computer for sending email, remember that your employer most likely has the right to monitor and perhaps even read your email when using work resources. Check with your supervisor if you have questions about email privacy at work.

An Easier Way to Manage Your Security Awareness Program

SANS Institute's new Advanced Cybersecurity Learning Platform (ACLP) makes deploying, maintaining, and measuring awareness programs easier and more effective. Learn more at <https://securingthehuman.sans.org/u/jGf>.

Resources

- Phishing Attacks: <https://securingthehuman.sans.org/ouch/2015#december2015>
- Little Bobby Comics: <http://www.littlebobbycomic.com/projects/week-52/>
- Daily Security Tips: <https://www.sans.org/tip-of-the-day>

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus

OUCH!

IN THIS ISSUE...

- What is the Internet of Things (IoT)
- Issues With IoT
- Protecting Your IoT Devices

Internet of Things (IoT)

What Is the Internet of Things (IoT)

In the past, technology was relatively simple; you just connected your computer to the Internet and used it for your daily activities. However, technology became more advanced when mobile devices came into our lives, devices such as smartphones and tablets. These devices put the power of desktop computers into our pockets. While far more mobile, these devices also brought their own, unique security challenges. The next big technical advancement is the Internet of Things. The Internet of Things, often shortened to IoT, is all about connecting everyday devices to the Internet, devices from doorbells and light bulbs to toy dolls and thermostats. These connected devices can make our lives much simpler; for example, having your lights automatically activate as your phone recognizes when you get close to home. The IoT market is moving at an amazing pace, with new devices appearing every week. However, like mobile devices, IoT devices also come with their own individual security issues. In this newsletter, we help you understand what those risks are and what you can do to secure your IoT devices, your home, and your family.

Guest Editor

James Lyne ([@jameslyne](#)) is global head of security research at the security firm Sophos. A self-professed 'massive geek,' his technical expertise spans a variety of the security domains. He is a certified instructor at the SANS institute and often a headline presenter at industry conferences.

Issues With IoT

The power of IoT is that most of these devices are simple. For example, you simply plug your coffee machine in and it asks to connect to your home Wi-Fi network. However, all that simplicity comes at a cost. The biggest problem with IoT devices is that many of the companies making them have no experience with security. Instead, their expertise is manufacturing household appliances. Or perhaps they are a startup trying to develop a product the most efficient, fastest way possible, such as on Kickstarter. These organizations are focusing on profits, not cyber security. As a result, many IoT devices purchased today have little or no security built into them. For example, some have default passwords that are well known, perhaps even posted on the Internet, and cannot be changed.

Internet of Things (IoT)

In addition, many of these devices have no option or ability to configure them; you're stuck with whatever was shipped. To make matters worse, many of these devices can be difficult to update or may not even have the capability. As a result, many of the IoT devices you are using can quickly become out of date with known vulnerabilities that cannot be fixed, leaving you permanently vulnerable.

Protecting Your IoT Devices

So what can you do? We definitely want you to leverage the power of IoT devices securely and effectively. These devices can provide wonderful features that can make your life simpler, help save money, and increase the physical security of your home. In addition, as the technology grows, you may have no choice but to purchase or use IoT devices. Here are some steps you can take to protect your IoT devices and yourself:



- **Connect Only What You Need:** The simplest way to secure an IoT device is to not connect it to the Internet. If you don't need your device to be online, don't connect it to your Wi-Fi network.
- **Separate Wi-Fi network:** If you do need your IoT devices online, consider creating a separate Wi-Fi network just for them. Many Wi-Fi access points have the ability to create additional networks, such as a Guest network. Another option is to purchase an additional Wi-Fi access point just for IoT devices. This keeps your IoT devices on an isolated network, where they cannot be used to harm or attack any computer or mobile devices connected to your primary home network (which is still the main interest of cyber criminals).
- **Update When Possible:** Just like your PC and mobile devices, keep your IoT devices up to date. If your IoT device has the option to automatically update, enable that.
- **Strong Passwords:** Change any passwords on your IoT device to a unique, strong passphrase only you know. Can't remember all of your passphrases? Don't worry, neither can we. Consider using a password manager to securely store all of them.

Internet of Things (IoT)

- **Privacy Options:** If your IoT device allows you to configure privacy options, limit the amount of information it shares. One option is to simply disable any information sharing capabilities.
- **Consider Replacement:** At some point, you may want to replace an IoT device when your existing one has too many known vulnerabilities that cannot be fixed or there are newer devices that have far more security built into them.

There is no one size fits all for every device, so it is worth checking for best practices and any publications on how to secure them. Unfortunately, most IoT devices were not developed with cyber security in mind, so many manufacturers do not provide much security information. But as awareness for cyber security grows, we hope to see more and more IoT vendors build security into their devices and provide more information on how to protect and update them.

Meeting NERC CIP Training Requirements

SANS has developed training for electric utility organizations subject to the NERC CIP Reliability Standards. Learn how SANS can help you meet the training requirements in NERC CIP-004 and CIP-003.

<http://securingthehuman.sans.org/u/gY8>

Resources

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](#). You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.org/ouch/archives. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org/gplus)

OUCH!

IN THIS ISSUE...

- What Is Encryption?
- What Can You Encrypt?
- Getting It Right

Encryption

What Is Encryption?

You may hear people use the term “encryption” and how you should use it to protect yourself and your information. However, encryption can be confusing and you should understand its limitations. In this newsletter, we explain in simple terms what encryption is, how it protects you, and how to implement it properly.

Guest Editor

Francesca Bosco ([@francibosco](#)) is a researcher and a project officer, managing projects related to cybercrime, cybersecurity, and the misuse of technology. She is working at the United Nations Interregional Crime and Justice Research Institute and she co-founded the Tech and Law Center.

You have a tremendous amount of sensitive information on your devices, such as personal documents, pictures, and emails. If you were to have one of your devices lost or stolen, all of your sensitive information could be accessed by whoever possesses it. In addition, you may conduct sensitive transactions online, such as banking or shopping. If anyone were to monitor these activities, they could steal your information, such as your financial account or credit card numbers. Encryption protects you in these situations by helping ensure unauthorized people cannot access or modify your information.

Encryption has been around for thousands of years. Today, encryption is far more sophisticated, but it serves the same purpose -- to pass a secret message from one place to another by ensuring only those authorized to read the message can access it. When information is not encrypted, it is called plain-text. This means anyone can easily read or access it. Encryption converts this information into a non-readable format called cipher-text. Today's encryption works by using complex mathematical operations and a unique key to convert your information into cipher-text. The key is what locks or unlocks your information. In most cases, your key is a password or passcode.

What Can You Encrypt?

In general, there are two types of data to encrypt: data at rest (such as the data stored on your mobile device) and data in motion (such as retrieving email or messaging a friend).

Encryption

Encrypting data at rest is vital to protect information in case your computer or mobile device is lost or stolen. Today's devices are extremely powerful and hold a tremendous amount of information, but are also very easy to lose. In addition, other types of mobile media can hold sensitive information, such as USB flash drives or external hard drives. Full Disk Encryption (FDE) is a widely used encryption technique that encrypts the entire drive in your system. This means that everything on the system is automatically encrypted for you; you do not have to decide what or what not to encrypt. Today, most computers come with FDE, but you may have to manually turn it on or enable it. It is called FileVault on Mac computers, while on Windows computers, depending on the version you have, you can use Bitlocker or Device Encryption. Most mobile devices also support FDE. iOS on iPhones and iPads automatically enable FDE once a passcode has been set. Starting with Android 6.0 (Marshmallow), Google is requiring FDE be enabled by default, provided the hardware meets certain minimum standards.

Information is also vulnerable when it is in transit. If the data is not encrypted, it can be monitored, modified, and captured online. This is why you want to ensure that any sensitive online transactions and communications are encrypted. A common type of online encryption is HTTPS. This means all traffic between your browser and a website is encrypted. Look for `https://` in the URL, a lock icon on your browser, or your URL bar turning green. Another example is when you send or receive email. Most email clients provide encrypted capabilities, which you may have to enable. A third example of encrypting data in transit is between two users chatting with each other, such as with iMessage, Wickr, Signal, WhatsApp, or Telegram. Apps like these use end-to-end encryption, which prevents third parties from accessing data while it's transferred from one end system or device to another. This means only you and the person you're communicating with can read what is sent.



Encryption is a powerful way to help secure your information, but it is only as strong as your key.

Encryption

Getting It Right

To be sure you are protected when using encryption, it is paramount that you use it correctly:

- Your encryption is only as strong as your key. If someone guesses or gets access to your key, they will have access to your data. Protect your key. If you are using a passcode or password for your key, make sure it is a strong, unique password. The longer your password, the harder it is for an attacker to guess or brute force it. Do not forget your password; without your key, you can no longer decrypt your information. If you can't remember all of your passwords, we recommend a password manager.
- Your encryption is only as strong as the security of your devices. If your device has been compromised or is infected by malware, cyber attackers can bypass your encryption. This is why it is so important you take other steps to secure your device, including using anti-virus, strong passwords, and keeping it updated.
- Many mobile apps and computer applications now offer strong encryption to protect your data and communications. If the app or application you are considering does not support encryption, consider an alternative.

Security Awareness Posters

Learn how to protect your family, friends, and coworkers with this series of friendly and free security awareness posters. Download the posters from <https://securingthehuman.sans.org/u/i58>

Resources

Encryption Explained: <http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/>

Passphrases: <https://securingthehuman.sans.org/ouch/2015#april2015>

Password Managers: <https://securingthehuman.sans.org/ouch/2015#october2015>

What Is Malware: <https://securingthehuman.sans.org/ouch/2016#march2016>

Securing Your New Tablet: <https://securingthehuman.sans.org/ouch/2016#january2016>

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



@securethehuman



securingthehuman.sans.org/gplus

OUCH!

IN THIS ISSUE...

- Your Wireless Network
- Your Devices
- Passwords
- Backups

Creating a Cybersecure Home

Overview

Several years ago, creating a cybersecure home was simple; most homes consisted of nothing more than a wireless network and several computers. Today, technology has become far more complex and is integrated into every part of our lives, from mobile devices and gaming consoles to your home thermostat and your refrigerator. Here are four simple steps for creating a cybersecure home.

Guest Editor

Matt Bromiley is an incident responder by day, where he helps clients of all sizes deal with data breaches. He is also a SANS instructor, where he teaches FOR508, the Advanced Digital Forensics and Incident Response course. Follow Matt [@mbromileyDFIR](https://twitter.com/mbromileyDFIR).

Your Wireless Network

Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables all your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. They both work the same way: by broadcasting wireless signals. The devices in your house can then connect via these signals. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

- Change the default administrator password to your Internet router or wireless access point. (Whichever one is controlling your wireless network.) The admin account is what allows you to configure the settings for your wireless network.
- Ensure that only people you trust can connect to your wireless network. Do this by enabling strong security. Currently, the best option is to use the security mechanism called WPA2. By enabling this, a password is required for people to connect to your home network, and once connected, their online activities are encrypted.
- Ensure the password used to connect to your wireless network is strong and that it is different from the admin password. Remember, you only need to enter the password once for each of your devices, as they store and remember the password.

Creating a Cybersecure Home

- Many wireless networks support what is called a Guest Network. This allows visitors to connect to the Internet, but protects your home network, as they cannot connect to any of the other devices on your home network. If you add a guest network, be sure to enable WPA2 and a unique password for the network.

Not sure how to do these steps? Ask your Internet Service Provider or check their website, check the documentation that came with your Internet router or wireless access point, or refer to their respective website.

Your Devices

The next step is knowing what devices are connected to your wireless home network and making sure all of those devices are secure. This used to be simple when you had just a computer or two. However, almost anything can connect to your home network today, including your smartphones, TVs, gaming consoles, baby monitors, speakers, or perhaps even your car. Once you have identified all the devices on your home network, ensure that each one of them is secure. The best way to do this is ensure you have automatic updating enabled on them wherever possible. Cyber attackers are constantly finding new weaknesses in different devices and operating systems. By enabling automatic updates, your computer and devices are always running the most current software, which makes them much harder for anyone to hack into.

Passwords

The next step is to use a strong, unique password for each of your devices and online accounts. The key words here are strong and unique. Tired of complex passwords that are hard to remember and difficult to type? So are we. Use a passphrase instead. This is a type of password that uses a series of words that is easy to remember, such as "Where is my coffee?" or "sunshine-doughnuts-happy-lost". The longer your passphrase is, the stronger. A unique password means using a different password for each device and online account. This way, if one password is compromised, all your other accounts and devices are still safe. Can't remember all those strong, unique passwords? Don't worry, neither can we. That is why we recommend you use a password manager, which is a special security program that securely stores all your passwords for you in an encrypted, virtual safe.



Follow these four simple steps to creating a cyber secure home: secure your Wi-Fi network, enable automatic updating, use unique passphrases, and enable backups.

Creating a Cybersecure Home

Finally, enable two-step verification whenever available, especially for your online accounts. Two-step verification is much stronger. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app on your smartphone that generates the code for you. Two-step verification is probably the most important step you can take to protect yourself online, and it's much easier than you think.

Backups

Sometimes, no matter how careful you are, you may be hacked. If that is the case, often the only way you can recover your personal information is to restore from backup. Make sure you are doing regular backups of any important information and verify that you can restore from them. Most mobile devices support automatic backups to the Cloud. For most computers, you may have to purchase some type of backup software or service, which are relatively low-priced and simple to use.

Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at <https://securingthehuman.sans.org/ouch>.

Resources

- Passphrases: <https://securingthehuman.sans.org/ouch/2017#april2017>
- Password Manager: <https://securingthehuman.sans.org/ouch/2017#september2017>
- Two-factor Authentication: <https://securingthehuman.sans.org/ouch/2017#december2017>
- Backups: <https://securingthehuman.sans.org/ouch/2017#august2017>

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](#). You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus

OUCH!

IN THIS ISSUE...

- Overview
- Five Simple Steps
- Securing Kids When Visiting Others

Helping Others Secure Themselves

Overview

Many of us feel comfortable with technology, to include how to use it safely and securely. However, other friends or family members may not feel so comfortable. In fact, they may be confused, intimidated, or even scared by it. This makes them very vulnerable to today's cyber attackers. Cyber security does not have to be scary; it's actually quite simple once you understand the basics. They most likely just need a guide like you to help them understand the basics.

Guest Editor

Randy Marchany (Twitter: [@randymarchany](https://twitter.com/randymarchany)) is the CISO at Virginia Tech and a certified SANS Institute instructor.

Five Simple Steps

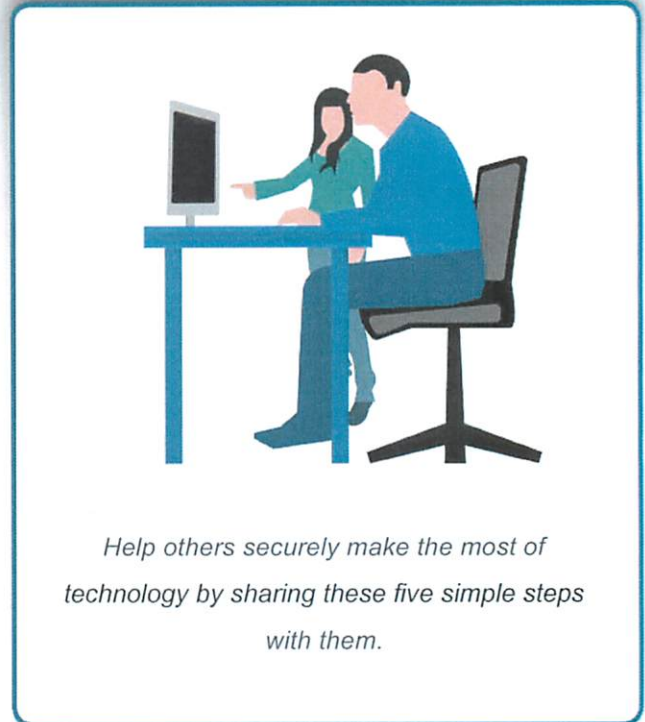
Here are five simple steps you can take to help others overcome those fears and securely make the most of today's technology. For more information on each of these points, refer to the References section at the end of this newsletter.

1. **Social Engineering:** Social engineering is a common technique used by cyber attackers to trick or fool people into doing something they should not do, such as sharing their password, infecting their computer, or sharing sensitive information. This is nothing new. Scams and con artists have existed for thousands of years. The only difference now is bad guys are applying these same concepts to the Internet. You can help others by explaining to them the most common clues of a social engineering attack, such as when someone creates a tremendous sense of urgency, when something is too good to be true, or when a cyber attacker pretends to be someone you know but their messages don't sound like them. Share examples of common social engineering attacks, such as phishing emails or the infamous Microsoft tech-support phone calls. If nothing else, make sure family members understand they should never give their password to anyone or allow remote access to their computer.
2. **Passwords:** Strong passwords are key to protecting devices and any online accounts. Walk your family members through how to create strong passwords. We recommend passphrases, as they are the easiest to both type and remember. Passphrases are nothing more than passwords made up of multiple words. In addition, help

Helping Others Secure Themselves

them to install and use a password manager. It is important to have a unique password for each of your devices and accounts. If a password manager is overwhelming, perhaps teach them to write their passwords down, then store those passwords in a secure location. Finally, help them enable two-step verification (often called two-factor authentication) for important accounts. Two-step verification is one of the most effective steps you can take to secure any account.

3. **Patching:** Keeping systems current and fully up-to-date is a key step anyone can take to secure their devices. This is not only true for your computers and mobile devices, but anything connected to the Internet, such as gaming consoles, thermometers, or even lights or speakers. The simplest way to ensure all devices are current is to enable automatic updating whenever possible.
4. **Anti-Virus:** People make mistakes. We sometimes click on or install things we probably should not, which could infect our systems. Anti-virus is designed to protect us from those mistakes. While anti-virus cannot stop all malware, it does help detect and stop the more common attacks. As such, make sure any home computers have anti-virus installed and that it is current and active. In addition, many of today's anti-virus solutions include other security technology, such as firewalls and browser protection.
5. **Backups:** When all else fails, backups are often the only way you can recover from mistakes (like deleting the wrong files) or cyber attacks (like ransomware). Make sure family and friends have an automated file backup system in place. Often, the simplest solutions are Cloud-based. They back up your devices hourly or whenever you make a change to a file. These solutions make it easy not only to back up data, but to recover it.



Securing Kids When Visiting Others

If you are comfortable with technology, you most likely not only have secured yourself, but helped secure your kids. However, when kids visit a relative who is not comfortable with technology, such as grandparents, these relatives may not be aware of how to best protect kids online or your expectations. Here are some steps you can take to help protect kids when they visit others, especially family:

Helping Others Secure Themselves

- **Rules.** Be sure that if there are any rules or expectations you have for kid's security, others know about them. For example, are there any rules on how long kids can be online, whom they can talk to, or what games they can or cannot play? Trust us, don't plan on kids explaining the rules to other family members. One idea is to create a 'rules sheet' and share that with any relatives your kids frequently visit.
- **Control.** If a child understand technology better than their guardians, they may take advantage of that. For example, kids may ask for or gain administrative rights to a grandparent's computer and then do whatever they want, such as installing that game you may not want them playing. Make sure relatives understand they should not give the kids any additional access beyond what has been established.

Finally, suggest to people that they subscribe to resources, such as the OUCH! newsletter, so they can continue to learn on their own. This newsletter is published every month for free in over 20 languages. Sign up at

<https://securingthehuman.sans.org/ouch>.

2017 Security Awareness Report

Learn the latest trends and lessons learned in building mature awareness programs from over 1,000 security awareness professionals. <https://securingthehuman.sans.org/report>.

Resources

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Backup and Recovery:	https://securingthehuman.sans.org/ouch/2017#august2017
Securing Today's Online Kids:	https://securingthehuman.sans.org/ouch/2017#may2017

License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](#).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit securingthehuman.sans.org/ouch/archives. Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplu

ABA Formal Op. 17-477

American Bar Association Formal Ethics Opinion 17-477

American Bar Association

SECURING COMMUNICATION OF PROTECTED CLIENT INFORMATION

May 11, 2017 Revised May 22, 2017

Formal Opinion 477R *

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for email communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."¹

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.²

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.³

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation. DPA1#At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."⁴ Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.⁵

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the “technology amendments” made to the Model Rules in 2012, identify some of the technology risks lawyers face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁶ The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment 8^o to Rule 1.1 was modified to read:

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. (Emphasis added.)⁷

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.⁸

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise.⁹ The 2012 modification added a new duty in paragraph (c) that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”¹⁰

Amended Comment [18] explains:

Paragraph (c) 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 1.1, 5.1 and 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 (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

At the intersection of a lawyer's competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology,” and confidentiality obligation to make “reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,” lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.¹¹

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.¹²

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a “reasonable efforts” determination. Those factors include:

- 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).¹³

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security

measures.¹⁴ Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.¹⁵ "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As Comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable

or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, “delete” usually does not mean information is permanently deleted, and “deleted” data may be subject to recovery. Therefore, a lawyer should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,¹⁶ and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.¹⁷ If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.¹⁸

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.¹⁹

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer's client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer's duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.²⁰

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and

- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”²¹ If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.²²

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.²³ The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment 19 to Model Rule 1.6, “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.”

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

1. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

3. See JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

4. “Cybersecurity” is defined as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” CYBERSECURITY, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/cybersecurity> (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that “[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information.” Ed Finkel, *Cyberspace Under Siege*, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

7. *Id.* at 43.

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.”

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: “[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances.”

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

14. See item 3 below.

15. See, e.g., Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/>.

16. See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

18. some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, See, e.g., Tex. Prof'l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

19. See *Veteran Med. Prods. v. Bionix Dev. Corp.*, Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

20. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

21. The ABA's catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethicschart.html.

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [4] (2016). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).
ABA Formal Op. 17-477