ZAFAR KHAN

TECH ESSENTIALS FOR THE MODERN INVESTOR

From cyber fraud and espionage
to practical tips for improving your security,
compliance, and productivity.

TABLE OF CONTENTS

FOREWORD

TECH ESSENTIALS FOR THE MODERN INVESTOR was written to open your eyes to the new world of big data, privacy risks, and Internet criminal tactics so that as an investor, you can make informed decisions as to what information you might want to share (or not expose), what software you might want to employ to increase your protection and take advantage of productivity opportunities with today's technologies, and to provide some insight as to what the future might look like.

Why should you care? We discuss how companies are siphoning off your personal, financial, and habitual information, using the information to build profiles on you, and then selling your profile to organizations that want to track, target, or market to you. Some people enjoy this as it gives them the opportunity to receive more targeted advertising in their email – but they are often not aware that Internet criminals can also use this information to target you with sophisticated cyber fraud and hacker attacks.

Today, Microsoft and Google are an extension of your life. With Google, it is impossible to avoid providing them your information if you use Google products (search, Gmail, document storage online). With Windows 10, unless you take great care when you first start using, every document you create is stored in a "Drive" in the Microsoft Cloud, where Microsoft discloses that they have the

right to read your information and analyze it. There is a mirrored document structure on your computer's hard drive and on the OneDrive (your Microsoft online drive). The copying of your information might be refreshing for those that want an instant backup… but do you really want all of your financial and personal information stored and analyzed by Microsoft, automatically? Microsoft Window 10 goes further with Cortana, for example, which can, perhaps without your knowledge, record your keystrokes, listen to your conversations and watch you via your built-in computer microphone and camera. Microsoft's Cortana is particularly invasive as this has access to your camera and microphone along with your contacts, calendar, keystrokes, web browsing history, web search key words, and all of your documents. Apple's Siri is similar, on your mobile device, and Amazon Echo listens to you in your living room. People have reported having conversations in their living room, only to receive email marketing messages related to those conversation topics soon after. Creepy.

This is all disclosed of course. Microsoft states, for example: We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary.

The good news is, with some awareness, you can learn how to use these powerful technologies (Windows 10, with all its built in "spying," is really built with the end user's convenience, needs and goals in mind). You can opt out of these features to enhance your privacy, but you need to know where to look. Windows 10, for example, has a Settings and Privacy applet, where you are greeted with 13 different screens to weed through, to opt out of things (read each carefully). Most of the concerning ones are on the General tab, but you really should go through all tabs, to understand and customize which types of data each app on your system can access.

With Apple's iPhone, within the Location Services area, you can see all of your physical locations visited and the tracking that is shared with Apple, other apps, and sometimes other people. For example, if you do not want a cumulative list of every physical location you have visited stored by Apple and shared with apps and marketers (among others), you might take the time to turn that "feature" off, hidden away in sub menus.

Some people simply claim none of this is important as their life is not interesting enough for others to care about enough to monitor their activity. Hackers like these people, as they can use legitimate marketing and social media tools (often back-end purchased premium accounts) to cull this data on you, run your profile through an algorithm to determine if you are worth targeting (if you have the financial resources to pay ransom to regain access to your personal files and photos, and if you are making investments) and then they lure you to send funds to hacker or imposter bank accounts.

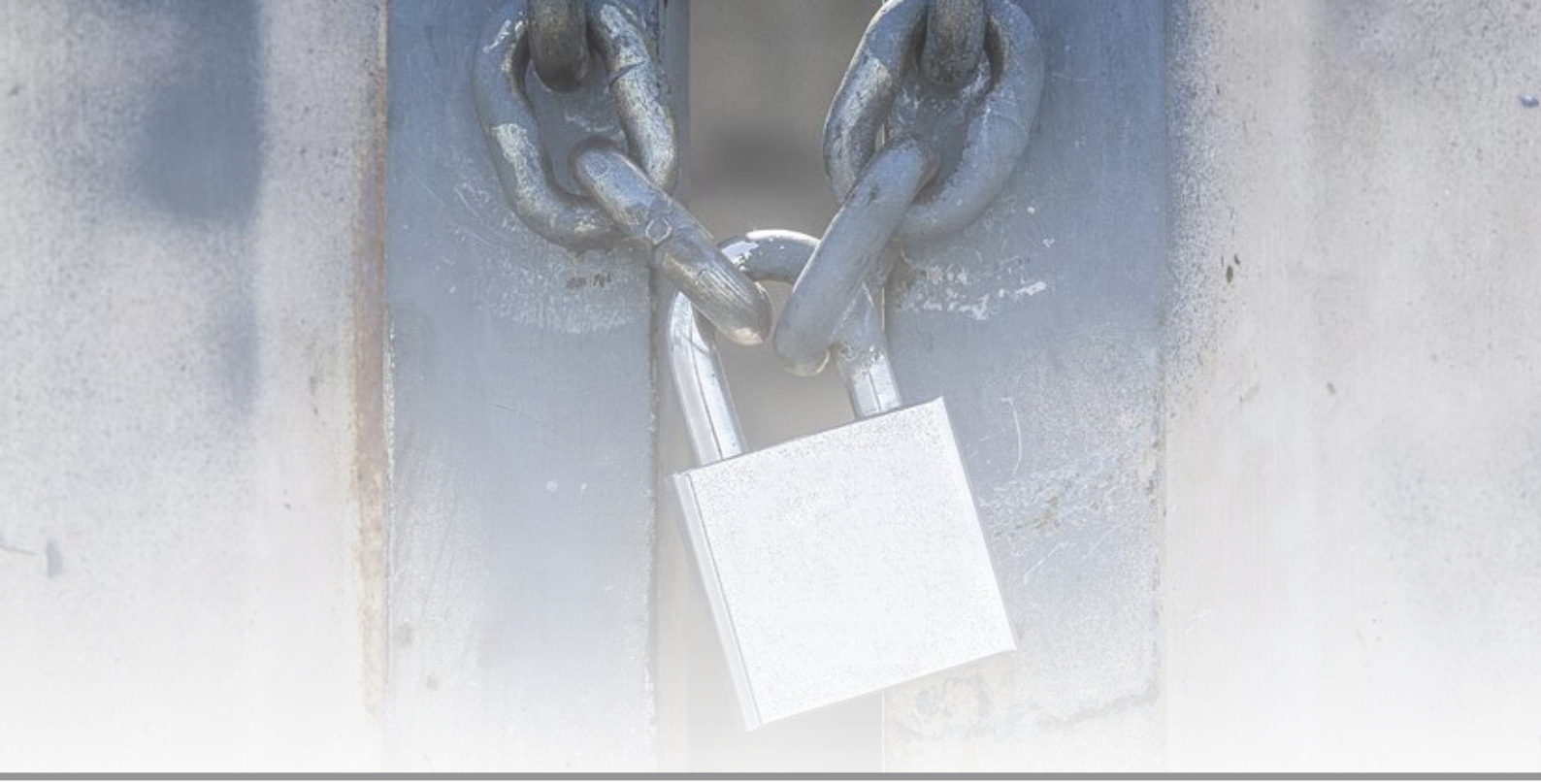
If you are an investor or investment advisor, your profile would certainly trigger the green light for hackers to target you.

This book aims to increase your awareness of these trends and threats, recommend tools you can use to protect and equip yourself, and show you how to meet these challenges head on.

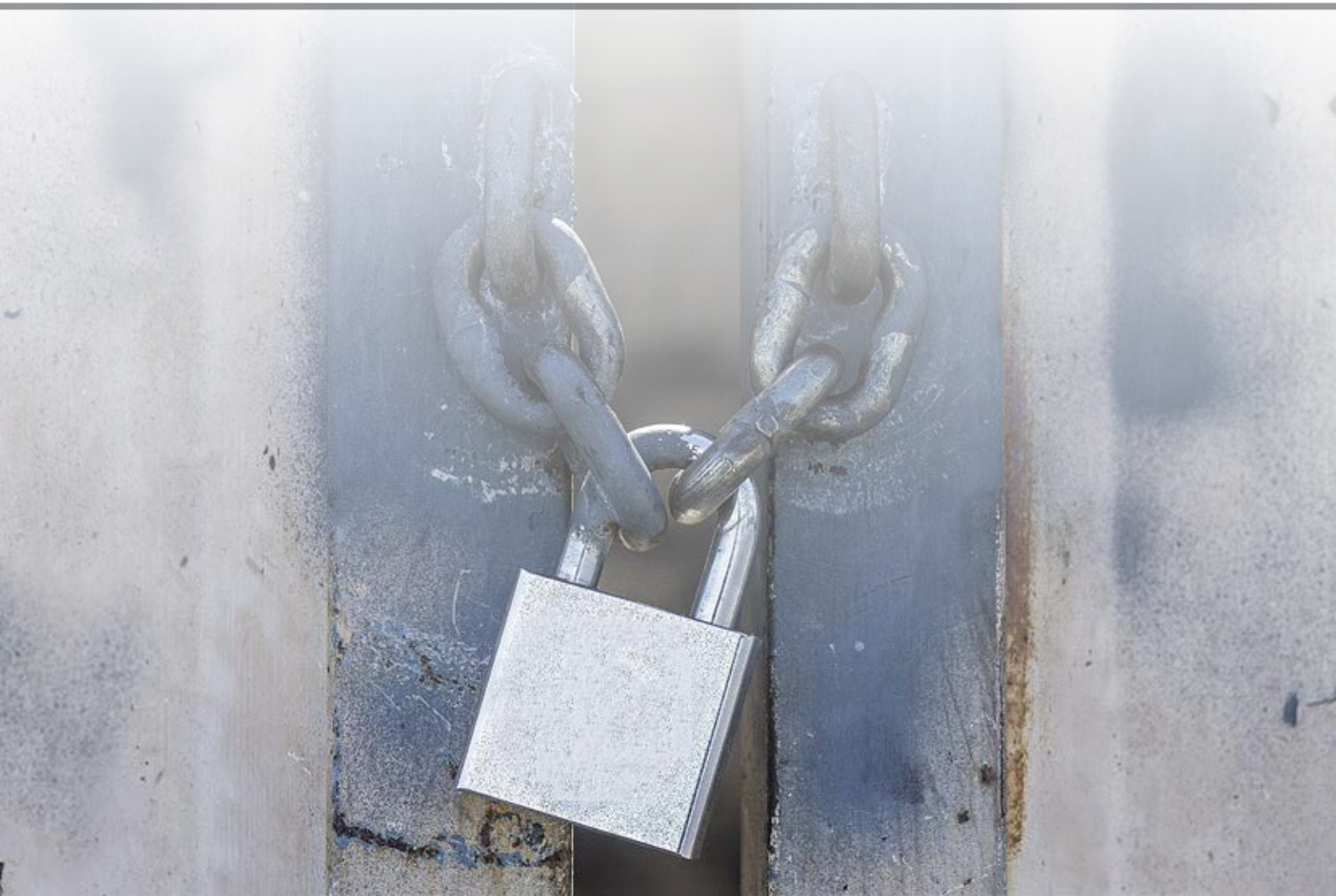
This book is just the beginning. To receive weekly *Tech Essentials* articles, subscribe for free at http://www.rpost.com/techessentials

Enjoy the book,

Zafar Khan



PRIVACY



RUSSIAN HACKERS & PIG LATIN

With the recent media focus on cybersecurity, whether it is talk of Russian hackers scheming to influence US presidential elections or "Brexit" votes, or the pervasive pressure to comply with HIPAA (healthcare privacy regulations) or other consumer data privacy requirements, "encryption" is one of the solutions that is often introduced.

When sending email, email encryption can indeed protect your strategic dialog from potential exposure, and its mere use can demonstrate your best efforts to protect consumer data against data breaches. As reported by The Guardian, NSA whistleblower Edward Snowden has said, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

Not all email encryption and methods of use are equally effective, though. And, one might prefer different types of encryption depending on the situation.

"Caesar Cipher" and "Pig Latin" are Forms of Encryption

Suppose Hillary wants to send a secret message to her friend Bill but worries that snoopy Vlad may intercept it. Hillary needs a way to scramble her message so that only Bill can read it. A simple way to do this would be for Hillary to replace each letter in her message with the next highest letter; shifting it by one (think "Caesar Cipher" or "Pig Latin").

But, of course, that is too simple. If Vlad intercepts the message, he'll be able to easily decipher it by looking for hidden patterns in the letters it contains. All it will take to crack the code is a little mathematics and a little trial and error.

And, of course, if Vlad uses a computer he'll be able to crack the code even faster. So, just shifting (as is the case with Pig Latin) the first letter to the end and adding "ay" as a suffix (turning "HELLO" into "ELLOHAY" for example) isn't a very strong cipher. Certainly Russian spies would crack this encryption. So, what can Hillary do?

Well, she can try to think up a more complicated mathematical formula to scramble the letters and numbers. And maybe she can use a computer to apply the formula. This will help, but the problem is that if Vlad hires clever mathematicians, or if he has a powerful enough computer, he will be able to crack the code eventually. So, it looks like it's going to be an arms race with Vlad to see who can come up with the biggest computers and the most complicated formula. But because Vlad has nearly unlimited resources to pay mathematicians and to spend on computing power, it is a race Hillary and Bill are perhaps bound to lose.

What is Considered "Strong Crypto"?

We have established that more complex encryption patterns are more difficult for Vlad to decipher, unless Vlad can use a powerful computer to help figure out

the pattern; yet they remain easy for Bill to read, because Bill has knowledge of the pattern (the decryption key). Most technicians understand that more complex algorithms are harder to "crack", that is, they require more computing power to crack.

How does Computing Power Impact the Time to Crack the Encryption?

Let's consider the example of using computing power to try to guess a 10 digit seemingly random alpha numeric password, such as: tjo9i0982d using a "Brute Force" attack (i.e. trial and error). This would be similar to trying to find a pattern in a universe of combinations of 36 digits (26 possible letters and 10 possible numbers). According to Gibson Research Corporation, in this example, there are 3700 trillion combinations, and the time to guess and test the right combination using trial and error in an online environment is one thousand centuries (assuming one thousand guesses per second). However, in what Gibson Research calls a "Massive Cracking Array Scenario" with one

hundred trillion guesses per second offline, this password can be guessed in just 38 seconds.

Computing power does matter. But, not many, if any (today), can implement a "Massive Cracking Array Scenario". One institution that could potentially implement such a system is the National Security Agency (NSA). In 2014, the NSA completed a $1.5 billion data center in Utah that reportedly has more than 100,000 square feet of computer and data storage equipment in a facility that spans a total of 1-1.5 million square feet.

Is Today's Commercial Encryption Readable by the Russian Spies with their Computing Power?

This is a question that some people know the answer to. We do not. Most commercial encryption uses algorithms that the NSA has "approved" for "civilian, unclassified, non-national security systems". These algorithms are what encrypt your email or financial transactions when using email encryption or secure HTTP web based connections with commercially available systems. Some of these NSA approved (unclassified) algorithms include DES, Triple DES, AES, DSA and SHA.

So, when it comes to using email encryption to protect "civilian, unclassified, non-national security systems" and information, what are the most important considerations? Continue reading "Preventing an 'Assange October Surprise'" to learn about some of the key considerations.

PREVENTING AN "ASSANGE OCTOBER SURPRISE"

Does your news feed closely resemble the plot of a Russian spy novel? It certainly might if you've been following the recent drama and mudslinging between the Democrats, the Russian government, the FBI, and the CIA, following the public release of private Democratic National Committee (DNC) emails. And that's before the warnings of an "October Surprise" promised by WikiLeaks founder Julian Assange. As you may know, Assange threatened to release more confidential emails before the November election. Who needs fiction?

We can't explain the media circus or separate their facts from fiction. But we can explain, in basic terms, the three main types of email encryption services available today, that can help protect your sensitive emails.

1. True Direct Delivery – Email encryption services that use "True Direct Delivery" wrap email messages in encrypted PDF files that are delivered directly to the recipient's inbox. This is a "strong crypto system"

because (a) the message content is not stored in the middle, (b) content is truly delivered to the recipients' desktops encrypted using AES 256 bit encryption, and (c) the content remains encrypted at the recipient end-point to prevent a potential breach. This is the method used in RPost's RMail service, and RPost has made it easy to send these from Microsoft Outlook, Gmail, and iPads, for both compliance and personal privacy.

2 **Secure Store and Forward** – This is a multi-step recipient retrieval process and it often leads to recipient complaints. This type of system stores your message content on a third party server and sends a link to the recipient to set up a username and password to download the content. Third party servers are often managed by a third party company with unknown security practices. Data can be hacked on the server before or after you access your message. Content storage duration is often unknown.

Store and Forward is also cumbersome. The last thing your clients need is to create another login and password, simply to access an email you've sent them.

3 **Public Key Exchange** – This is a secure system that is extremely complex. The organizations that use this method include the Department of State and the Department of Defense. It is secure but very complicated to use when communicating with external parties. Public Key Exchange involves exchanging public encryption keys among contacts (PKI Digital Certificates). Users have to purchase and install digital certificates, manage the expirations, ensure their recipients have exchanged public keys, and use a compatible email program such as Microsoft Outlook desktop software. If you are sending messages to a client and they do not have their own public key, the system won't work.

The best way to enforce a secure messaging system in your office is to select a "strong crypto system" that makes it easy for both senders and recipients to protect sensitive message content and file attachments. For many, the ease-of-use of True Direct Delivery-based services such as RMail is a deciding factor.

GOOGLE HAS AN EASIER WAY TO READ YOUR EMAIL

Take Google as an example with your laptop as the endpoint. Google allegedly provides information to NSA and other government organizations upon request, and also perhaps others, depending on how you interpret what they disclose on their website privacy policies. (A quick glance at Google's privacy policies are revealing.) Google discloses: "Local storage: We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches" and further "may combine personal information from one service with information, including personal information, from other Google services."

With all of the hype about NSA computing power, we believe endpoint security should be of greater concern – Google is telling you (based on our interpretation of their privacy policy disclosure) that they record, analyze, cross reference your personal information, not only what you type into a Google application,

but potentially all application data that is stored on your device (the endpoint) that they can access using their techniques.

So, for example, if you take great care to type your email in a Gmail compose page, encrypt the transmission, and then send, you are forgetting that Google may be recording, storing, analyzing, and cross referencing the content of the message you type before you encrypt it (as well as perhaps other personal information on your computer or mobile device).

So, for those encrypting for privacy, endpoint security should be evaluated. Note, you can somewhat control your endpoint security by choices you make, but what about the encrypted email recipient's endpoint security?

If you are also interested in keeping your information private from Google and those that Google sells your information or profile to, move away from Google email (and Microsoft, AOL, and Yahoo) to the RMail Inbox product, or a smaller third party email provider and download your email to Outlook desktop software inbox for reading; and "Send Registered" in either case, using RMail.

RMail Inbox is a full featured web accessible email account with calendar, contacts, drive online file storage and sharing, spreadsheet and document viewing online with collaboration, email encryption, e-signatures, Registered Email certified e-delivery, email open tracking, and more. Users set up their account as Name@Rmail.com.

RETAILERS ARE USING YOUR ONLINE ACTIVITY TO MAKE YOU PAY MORE

In recent briefings, we have reported on Internet criminals' behavior with regards to researching their victims' professional profiles and associations (using LinkedIn recruiter tools, for example) and using these social cues to lure unsuspecting victims into sending money to imposter accounts.

Even if you have not been targeted in this way, if you use online shopping websites or web-based email services like Gmail, your online activity is constantly being recorded and used by retailers and marketers to extract the maximum amount of revenue contribution from you.

Often, your online activity feeds these retailers data that allows them to target you with a price manipulation scheme called "price discrimination", whereby you will be subjected to a different price (either higher or lower) than others viewing the same exact product or service online. This method of showing different shoppers different prices for the same product at the same time based on information a retailer knows about a shopper (price discrimination) is legal.

The idea of being discriminated against based on socio-economic and behavioral data online is unsettling to many. A phone survey conducted by the Annenberg Public Policy Center of the University of Pennsylvania reported that 76% of respondents agreed that "it would bother me to learn that other people pay less than I do for the same products."

Websites change prices based on many types of data points: customers' online habits, words that appear in email in their Inbox, browser type, the type of device they use (i.e. iPhone, Android, Mac, PC, version), operating system, login status, time spent on online watch/preorder lists, geography, other websites visited, search term history, time of day, offline shopping habits (such as data from store loyalty programs), and more. If you have location services enabled on your device when you are browsing a web store, your device's geo-locator may tell the e-tailer your location, which they may use to offer you different pricing.

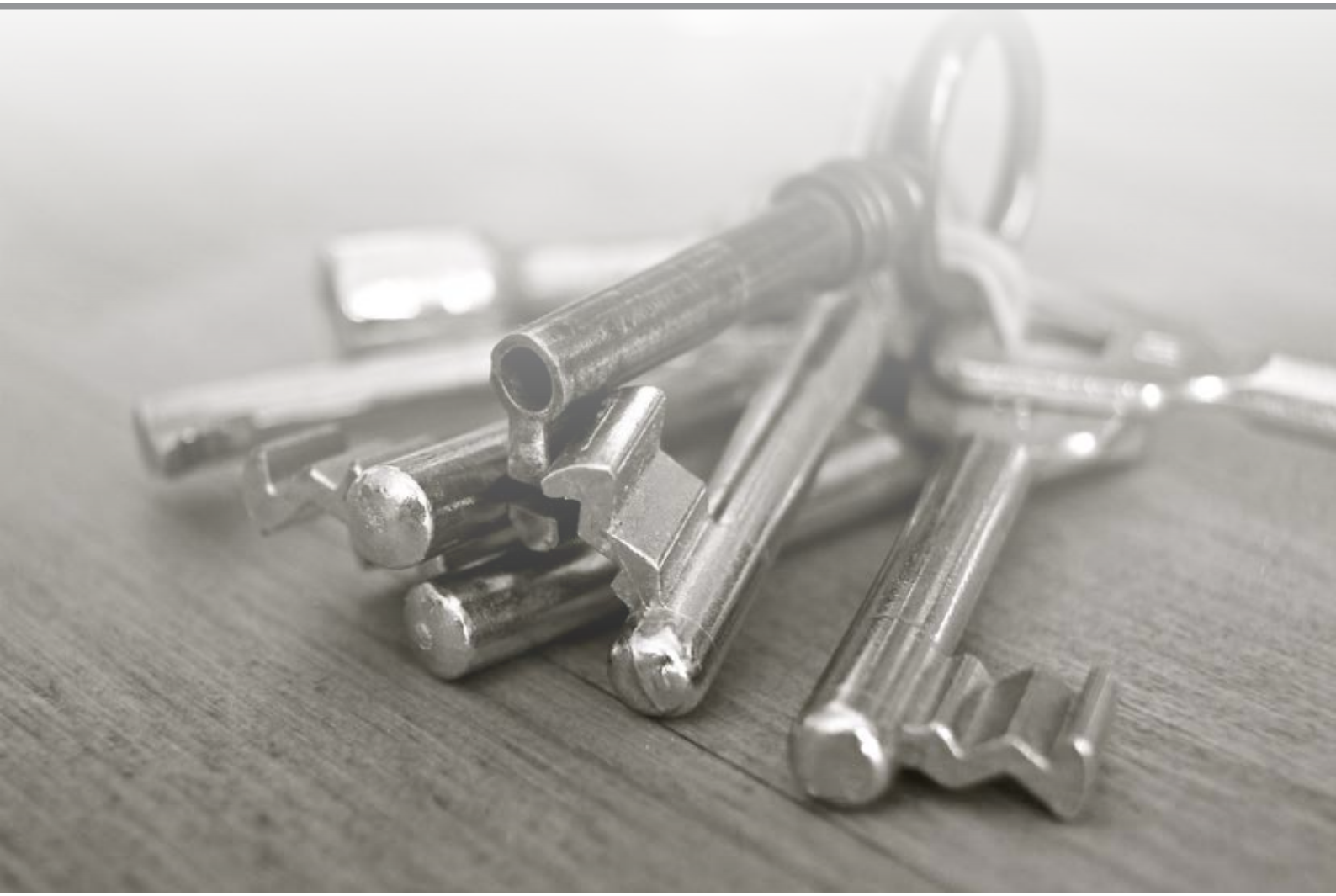
Northeastern University recently published a comprehensive study across commonly used retail websites. As an example of their findings, Home Depot shows shoppers higher pricing (relative to brick-and-mortar prices) if they search using a mobile device, and even higher prices if the mobile OS is Android. Why might they do this? Perhaps it is to give their customers greater satisfaction from going into a store, checking a price using their phone, and discovering that the item in their hands is a great deal, leading to a higher probability of a purchase.

Some companies will charge you more if you are a Mac user. Why? Perhaps they assume that Mac users pay more for their computers and therefore have a higher "willingness to pay" for other goods and services. Orbitz executives, for example, confirmed to the Wall Street Journal, that the company had "experimented" with showing different hotel offers to Mac vs. PC visitors.

In light of these sophisticated price discrimination tactics, what can you do to gain more control of your online shopping experience? Try deleting your browser cookies and logging out of any online accounts before an online search, if you believe that your behavior profile may be used against you. Use time to your advantage. When you put an item in your shopping cart, but abandon the cart without buying, some online retailers will cut the price to close the deal.

Assume your online behavior is tracked. Also, assume the content of the email in your recipient's inbox is automatically culled and associated with you (if you send to an @ Gmail, Hotmail, Outlook.com, MSN, Yahoo, AOL, or other similar email address). Note, a simple way to prevent your email content from being culled is to use RPost's Inbox Secured executive mode email encryption.

SECURITY



THE ULTIMATE SECURITY DILEMMA

In a society that embraces online shopping, GPS location tracking, mobile texting and email anytime and anywhere, it is no wonder that technology's promise of convenience continues to overrule many peoples' instincts to protect and secure their private information.

The preference for convenience over security is present even at the highest levels of the US Government. With the news earlier this year about former Secretary of State Clinton succumbing to the temptation of using unsecure personal email for official state business – it is not surprising that many investors often click the "send" button with sensitive investment-related or personal information attached, hoping or assuming that the emails reach their destination fast enough to avoid being intercepted.

Well, the email is transmitted fast, but never fast enough to prevent "un-friendlies" from siphoning its message contents from the electronic trail it leaves behind.

The constant challenge for IT professionals and security experts is to balance security and usability. If the most secure system is too complicated or cumbersome to use, people will circumvent it – as Secretary Clinton did. Once the official or corporate system is circumvented, security devolves from professional (IT executive) to amateur (end user).

Secretary Clinton's use of a personal email system purportedly set up in her house by a colleague is a perfect, high profile example of this – but certainly not an isolated example. It has now been reported that Defense Secretary Ashton Carter used his personal email account to conduct official government business early in his tenure at the Pentagon, using personal email installed on his iPhone, rather than a secure professional account.

"With all the public attention surrounding the improper use of personal email by other Administration officials, it is hard to believe that Secretary Carter would exercise the same error in judgment," remarked Sen. John McCain (R-Ariz.), Chairman of the Senate Armed Services Committee.

IT professionals often underestimate just how simple the user experience must be for widespread adoption. When the recipient says to the sender, "just send the darned thing," because they get frustrated with the more secure process, the sender often just sends it, concerned that they are annoying the recipient with some policy or "process" IT has put in place.

If it is not simple to use, people will circumvent the process; and they do – even those who know they shouldn't, like the former US Secretaries of State and Defense.

THE BIGGEST THREAT TO YOUR ONLINE SECURITY COULD BE YOUR PASSWORD

Email security has been a hot topic as of late, with recent news of a supposed breach of 272 million email usernames and passwords and recent statements made by a hacker who claims to have accessed Hillary Clinton's private email server two years before the private server's existence was first reported by the New York Times. In the latter story, the hacker known as "Guccifer" claims he correctly guessed Clinton confidant Sidney Blumenthal's AOL password and used the hacked email account as a stepping stone to Clinton's private email server.

These stories highlight the fact that weak passwords continue to be the entry point of choice among hackers and cybercriminals. A weak email password can easily be guessed or even cracked by password-cracking tools that are freely available online, providing hackers access to all the victim's emails, which can in turn compromise other accounts and sensitive information.

To help shore up what could be the biggest threat to your online security, here are ten best practices for your online passwords:

- Do not use passwords based upon personal details that can be easily discovered, such as birthdate, social security number, phone number, or a family member's name.
- Do not use words that can be found in the dictionary. Password-cracking tools routinely use dictionary lists to try to crack passwords.
- Do not use the word "password" as your password. (Many still do!)
- Try not to use "!", "1" or "9" when required to add a symbol or digit, as these are easily guessed by hackers.
- Create unique passwords that use a combination of words, numbers, symbols, and both upper and lowercase letters.
- Avoid using adjacent characters on a keyboard. For example, "qwerty", "asdzxc", and "123456" are very easy to crack.
- Length is key. These days, it's very affordable to build powerful and fast password cracking tools that can try tens of millions of password combinations per second. Each character you add to a password makes it an order of magnitude more difficult to crack via brute force methods.
- Avoid using the same password at multiple websites. It's generally safe to use the same password at sites that do not store sensitive information about you.
- Do not use your email account password at any online site. If that site is compromised, your email account will also be compromised.
- Do not store your password list on your computer in plain text. Either write your passwords down (and keep them out of view) or use a local password storage program, which can protect all your passwords with a single master password.

A single compromised email account can provide a cybercriminal with the valuable social cues and background information they need to perpetuate a successful and highly profitable cyberattack. Yet, besides monetary incentives, it is also believed that many hackers hack online accounts for bragging rights or out of a need to feed their egos. In the instance involving 272 million compromised email accounts, the hacker allegedly offered to sell account credentials for just

50 roubles, or less than $1, and eventually agreed to trade the information in exchange for favorable comments posted on an online hacker forum.

A strong password strategy is essential to maintaining email privacy, but it's also just the beginning. To maintain email privacy when sending sensitive or personal information, you need to use an email encryption service. RMail, for example, contains an easy-to-use email encryption feature that provides true direct delivery of encrypted emails and does not require recipients to install any software or register for any accounts.

Will Biometric Data Replace Passwords?

Many companies are continually struggling to protect customer data from hackers, thieves and other cybersecurity threats. Some firms have begun using biometric data in place of passwords. For example, many banks now allow customers to use fingerprint or iris identification to access bank accounts from mobile devices. This includes Bank of America, JP Morgan Chase and Wells Fargo. Google and other technology firms are working to combine biometric information to further strengthen security using information such as eye scans, fingerprints, face shape, voice recognition and even body movement. The prevailing idea is that although a single biometric indicator would not be secure enough by itself, a combination of many such indicators could "result in something more than 10 times as secure as a fingerprint." And an ancillary promise is that biometric-based security would afford the ultimate in convenience to end users, who would no longer face the challenge of remembering convoluted passwords of their own creation.

While biometric-based security may be promising and is certainly attractive to institutions and individuals that require more effective cybersecurity, the promise of greater security could also be accompanied by new threats to personal privacy. Could consumers' fingerprints, iris scans, and other biometric data be shared with third parties, just as their demographic and certain behavioral data already is? For example, it is already legal for a cellular carrier to track and store your movements with cell-site location data.

If consumers share their biometric information with a cellular carrier or a bank, how might this data be used? Would banks share your physical characteristics with advertisers? Would a thief be able to use your biometric information to apply for a credit card? How far removed are we from a world where DNA verification is needed for such applications? Like any new technology, there are a myriad of considerations that materialize when you consider real world implementation.

As biometric-based security sees greater adoption, it is certain that criminals will attempt to steal this data. However, rather than lifting fingerprints off a beer bottle or lopping off a target's fingers in the audacious manner of a Hollywood film, hackers will seek out the digital representations of this biometric data on corporate servers, perhaps using malware to gain access to such data.

It will likely take many years for biometric security technology to be implemented throughout society due to the complexity of the aforementioned and other potential ripple effects. Before technologists and the corporate entities they serve are able to deliver on their promises of a biometrically-secured future, businesses must take advantage of presently available tools to protect themselves and their customers.

What are the security tools of today? For Internet banking, multifactor authentication with a temporary pin (tied to phone/email access), security question, or other secondary factors (used in combination with a robust password) is one well-known best practice for securing Internet banking accounts. For email, email encryption is recommended by security experts to maintain the privacy of your email message and any file attachments. While these practical cybersecurity solutions may seem less interesting than retina scans and motion-detecting sensors, they surely are the best available tools for the job – at least for the time being.

IS "SECURITY BY OBSCURITY" AN OBSOLETE CONCEPT?

The term "security by obscurity" has been around for a long time. Traditionally, this has referred to the idea that the best way to keep a system safe is to keep its design (and any potential vulnerabilities) a secret. To many, "security by obscurity" has also represented the idea that there is safety in numbers, such as on a social media network that has hundreds of millions of users. One might argue that the intersection of social media, online platforms that gather and sometimes sell (for legitimate purposes) personal data, and peoples' addiction to electronic communication convenience, may call for a new way of thinking about one's own (or a client's) security by obscurity.

Consider how the most prominent targets are being hacked

Sure, there are news stories of hackers targeting large companies – a recent one is a report of a Russian hacker targeting 48 major law firms focused on mergers

and acquisitions with the aim of gaining pre-public information to trade on in advance of news announcements. This hacker targeted hardened corporate IT departments, but there are certainly easier targets available.

For most hackers, the easiest target is you, the business user

Today, hackers can easily use sophisticated data mining techniques to target YOU, an individual email user. Hackers sometimes purchase personal data from marketing companies, multiple listing services, real estate platforms, and LinkedIn business recruiting tools (“See full profile details on any LinkedIn member, zero in on the right person with 20+ Premium search filters…” — LinkedIn) for back-end access to study a target’s job title and relationships, Facebook or Google data, and more. One tactic for the more experienced hacker is to set up fake companies to subscribe to tools that title insurance companies and credit departments legitimately use to learn about your financial dealings.

Recently, hackers have been successful at this type of attack -- which the FBI calls “Business Email Compromise” (BEC) and security experts call “whaling” or “spear phishing” -- to the tune of more than $1.2 billion reported stolen in average increments of $6,000 from individuals and $130,000 from businesses, according to the FBI.

2016 may be the beginning of the “Hacker Goldrush”

Once a hacker identifies his list of targets, it is not hard for him to gather the information required to trick someone into sending money to the hacker’s imposter bank account. The target may be someone who saved their money for years to purchase a new house, a lawyer or other trusted client advisor, a realtor, an insurance broker, a registered investment advisor or an accountant.

New targets and new tactics are identified every day

The latest scheme uncovered and reported by The Guardian, is based on a flaw in the underlying Signaling System No 7 (SS7) mobile communications protocols. With a little technical sophistication and the mobile phone number of the hacker’s target, the hacker can listen in on telephone calls, siphon off photos and other text messages sent and received, and track a target’s location.

To identify targets, the hackers often monitor the professional advisors as individuals (not even bothering a hack into their corporate networks like what was reported to happen with the Panama law firm Mossack Foncesa). The information gleaned may lead to other hacker opportunities, in terms of selling (or exposing) the data to regulators, adverse parties in litigation, or threatening to expose it and asking for ransom. All of this has consequences that attorney-client privilege arguments do not protect against. The US government, for example, has announced it will use the hacker-leaked data from the firm Mossack Foncesa, to initiate investigations against certain people.

What can you do about all of this?

There is not one single solution. One major recommendation is to use email encryption when sending sensitive personal or business information. However, the most important defense may be to simply take the time to learn a little about what is happening in Internet security and to use those tools that make it easy to maintain privacy and security when using the Internet and email.

PRODUCTIVITY

LEASE VS BUY – FIRST CARS, NOW SOFTWARE

When it comes to getting a new car, one of the first decisions many consider is whether to buy or lease. Of course, there are pros and cons to either approach. Buying a car means you own it (and perhaps get positive feelings about owning it), and you have more freedom over its use; you aren't subject to mileage restrictions, for example. But, buying a car is a significant financial commitment and could make changing cars impractical, at least before the car is either sold or becomes inoperable. For those who don't want to stay locked into the same vehicle for many years, prefer a simpler transaction, or prefer to always have the latest model, leasing is often more attractive than buying.

Always having the latest model, with minimal up front financial commitment, is what transformed the wireless phone industry into a (somewhat disguised) lease model. If you commit to a two-year service plan, your phone device payment is included in that plan, and you can renew your model every two years.

In recent years, the software industry has also begun to move to a "lease"-based model of software distribution. One popular product that has shifted to this distribution model is Microsoft Office.

In the past, and perhaps even now, your company's IT team may have purchased a specific edition of Microsoft Office (2010 or 2013, for example) on a CD or DVD-ROM, with unique serial numbers for each installation. This software purchase would have been expensive — $500 per install key, for example. To upgrade Microsoft Office for an entire team of 20 people would have cost more than $10,000 at once, a hefty-enough price tag to dissuade the least frugal of IT managers from making much-needed upgrades.

"Leasing" software, on the other hand, allows continual access to the latest and greatest version of a company's product, not to mention the productivity gains that come along with that. Companies prefer this as they believe that if customers have the latest version of their software, customer satisfaction will be higher and competitive risk lower.

Google, for example, makes its "Apps for Work" software available via a similar "leasing" model. (RMail has a Gmail add-in that is compatible with Google business email.)

Microsoft calls this new way of purchasing Microsoft Office its Office 365 product, the idea being that with this service, you always have the best version of Office, 365 days a year. As with car leasing and phone companies, the ultimate goal for companies like Microsoft is to make it easier for end users to continually have access to the best product, thereby increasing customer satisfaction and loyalty.

When purchasing Office 365 in this way, you still have the full installation of Office loaded on your computer or device. The latest version not only includes classic productivity tools such as Outlook, Word, PowerPoint, and Excel with a modernized user experience and feature set, but also new productivity-enhancing services such as OneNote and OneDrive, with online and mobile access. Newer versions of Office also have greater compatibility with 3rd party apps and add-ins that provide enhanced security, compliance, and productivity – such as RPost's RMail add-in for Outlook, which is also purchased with a small monthly fee.

HOW TO SEND LARGE FILES BY EMAIL

You may have noticed that when you send a large file attachment by email, it sometimes gets kicked back to you undelivered with an error message that says something like: “The attachment size exceeds the allowable limit.” But what are these limits? And how can you securely send a large file attachment when it’s too large to send by standard email?

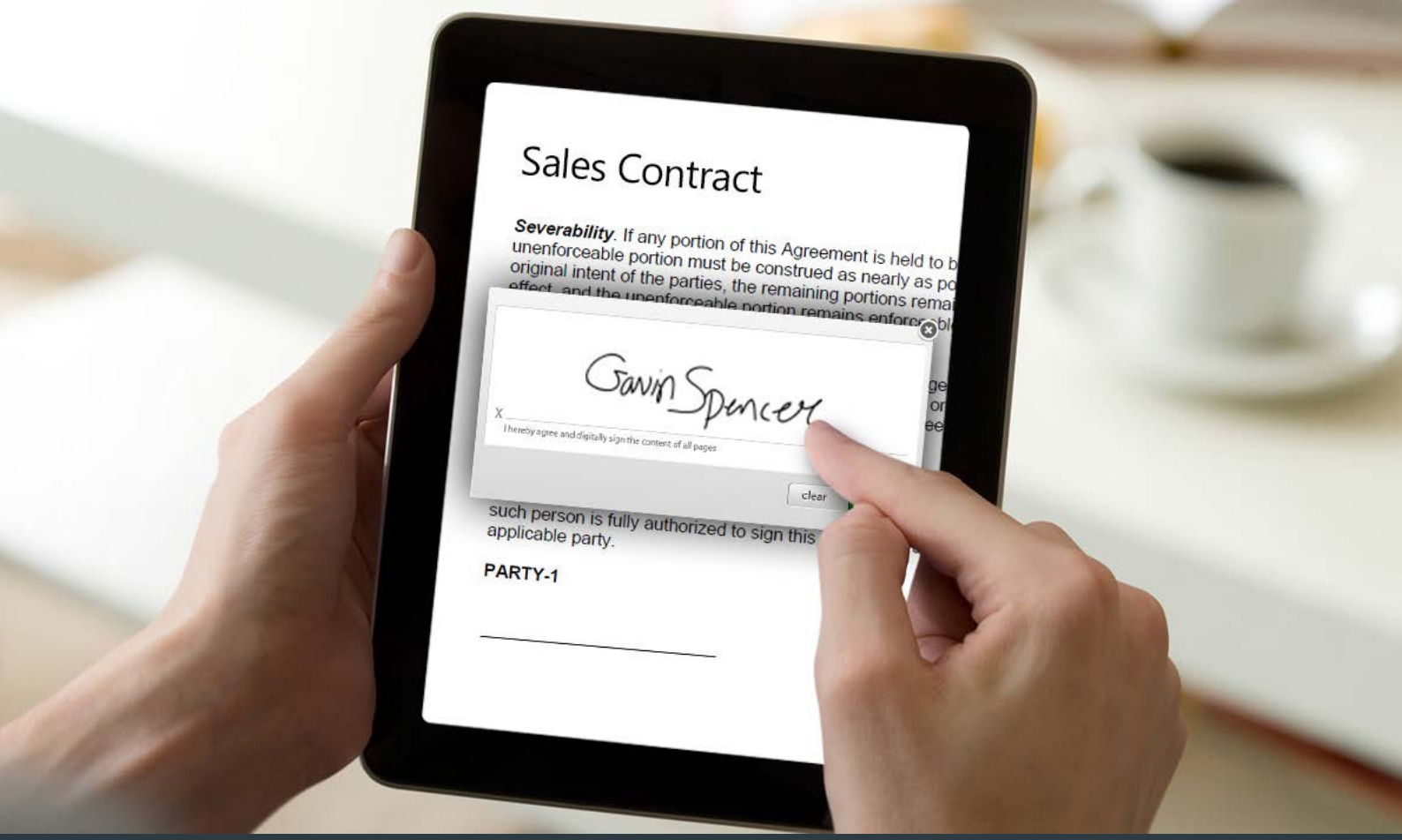
Most email providers enforce file size limitations on email attachments. For example, both Gmail and Yahoo limit file attachment size to a total of 25 megabytes (MB). Microsoft Outlook, the most widely used email client software, also includes file attachment size limits; Outlook 2010 and 2013 have a default attachment size limit of 20MB. Although these client-side limits can be changed or disabled, if your outbound message and attachments exceed either your or the recipient mail server’s size limits, the message will not be delivered and you will receive a non-delivery report (NDR) indicating the failure.

Because of these limitations, many professionals feel like they are forced to look beyond email if they wish to send large files or sets of files electronically. For example, a paralegal might "share" case files with his/her attorney using a file sharing service like Dropbox. A real estate agent might send closing documents using a file transfer website like Box.com. And an insurance agent might transfer an application to the carrier using an FTP server.

Many of these solutions entail significant drawbacks. (See an analysis comparing several competing solutions.) Some are not secure, making it possible to have your files be intercepted en route or accessed at rest from a recipient's inbox. File transfer sites typically store files on a third party server with varying and sometimes unknown levels of security. How long are they keeping a copy of your files? Is the data being stored in the US or abroad?

And even if a file transfer service is "secure," is it convenient? Most of the well-known file transfer services do not allow you to send large files from your Outlook email compose window, for example.

There is a simple solution for those that require a secure, email-based method for sending large files. Included in RPost's RMail service is the LargeMail™ file transfer feature, which allows you to send files up to 1GB from your email compose window. LargeMail™ can be used with RMail's encryption feature to ensure privacy.



ARE E-SIGNATURES LEGAL?

People use e-signatures every day without even realizing they're "e-signing" — signing on an electronic pad at grocery store check-out, replying to an email with a typed confirmation of terms, or putting in a PIN code for a debit card transaction, for example. Most people have no doubts about the legality of these everyday "e-sign" transactions.

Yet, according to a member poll of the International Association of Commercial and Contract Managers (IACCM), 71% of respondents identified "comfort with the legal process" as the most important consideration in their e-signature initiatives.

Surely e-signatures are legal, with professionals in all regulated industries now using them for their most critical transactions. But what makes e-signatures legal? To answer that question, let us first ask a different one. What is the purpose of a signature (whether electronic or not)? It is to provide a mark that is familiar to the signing parties that reminds them of what was agreed to. Con-

sidering this, in the United States, Canada, Singapore, the United Kingdom, and other countries, e-signature laws for most commercial transactions define legal electronic signature as a sound, symbol or mark; made with intent to sign, logically associated with the content.

While showing the mark (i.e. typed name in email) with a phrase indicating the intent to sign (i.e. typed "I agree" in the email) placed in line with email body text or referencing attachments (logically associated with the content) may constitute a "legal e-signature," there are situations where simply having a legal e-signature is not enough. In the event of a dispute, there is tremendous value in having a record of e-signoff that has high evidential weight and that can later be authenticated to provide forensic evidence of who signed what, when. (Remember, most electronic documents and email, regardless of form, can be altered with photo, PDF, or email editing tools, so a printed record may be easily challenged.)

For example, this forensic record may associate the signoff with Internet Protocol (IP) records to an individual' computer, associate the content of what they signed (using hashes, whether or not salted) to the signoff mark, and create a uniform timestamp that associates the content signed to a time of signoff.

An example of an e-signoff record with high evidential weight is the Registered Receipt™ record generated by RMail after sending and signoff. This is an evidentiary record that is returned to the sender by email, providing certified proof of delivery, content, time received, sending and receiving party, recipient signoff timestamp, audit trail forensics, and other key transaction details. This record is portable, so that in the event of a dispute, it can be forwarded by email to any opposing party, counsel, arbitrator, mediator or judicial officer, allowing that party to easily authenticate the transaction details.

COMPLIANCE

UNDERSTANDING COMMON MISCONCEPTIONS ABOUT PROVING EMAIL DELIVERY

Have you, your staff, or a client ever sent an important email that the recipient claimed he or she did not receive?

Here are several of the most common misconceptions about email delivery that will prepare you in case delivery of your (or a client's) time-dependent email is disputed.

1 I did not get a bounce notice, so I know my email got there.

This is a false assumption.

Why? Email technologists estimate that more than half of recipient mail servers do not return bounce notification emails.

In case you are curious why some mail servers are configured to not return bounce notices, here is a slightly technical explanation. Spammers

often send spam relayed through unknowing ISP mail servers to every conceivable iteration of "yourname@yourfirm.com". They will use automated systems to send to y.name@yourfirm.com, your.name@yourfirm.com, your.n@youfirm.com, and so on. Since most of these are not real addresses, your firm would be sending thousands of bounce notices back to unknowing sending ISP servers if your firm's mail servers were configured to send bounce notices. The sending ISP servers would then believe your firm's servers were sending it spam, possibly resulting in your firm's email servers getting blacklisted. Your firm's legitimate email would then simply disappear (before reaching the recipients) until your IT staff cleared up the blacklisting issue. This phenomenon is called "back-scatter blacklisting".

2 I copied (cc'd or bcc'd) myself and got the copy – so I know my message was delivered to all recipients.

This is a false assumption.

Why? Receipt of internal email within the organization does not have any bearing as to whether or not the email got to the Internet – and certainly does not prove delivery.

Here is a technical explanation of why that is the case. In most cases, if the sender and recipient have the same email domain (the domain being "@yourfirm.com"), the email will never need to transmit from your mail server to the Internet to reach the recipient. The email will travel from your computer to your mail server, and then, if your mail server sees the recipient domain as its own, it will look up the recipient in its own local directory, and put the email into that recipient folder (mailbox) locally on the mail server. The email will not need to be transmitted to the Internet to reach the recipient.

In the case where you copy yourself (or staff) on the message going to an external party, the message to your (and your staff) will remain on your mail server, and the message copy for the external party will trans-

mit to the Internet. Whether it is delivered will be dependent on a number of Internet delivery variables, but delivery success is independent of whether or not you (or staff) received their copy.

3 I copy my assistant and he/she prints a copy (to paper or PDF) for the file. This protects me in case I need to irrefutably prove who said what when at a later time.

This is a false assumption.

Why? Your printed copy can certainly remind you of what you believe occurred, but a printed copy is not proof of what actually transpired and can easily be disputed. It is incredibly easy to alter the content and time-stamps on an email and print it so that it appears authentic.

If there is a question of authenticity, the printed email (or PDF) can easily be denied admission into evidence. No matter how authentic your printed copy is, the recipient can simply claim non-receipt. If your printed copy includes the recipient's reply text and email thread, and the recipient's copy (the sender of the reply) does not match, it will be challenging to prove which one is authentic.

4 I save everything in my archive, sent folder and/or inbox. I therefore can prove when they got my email and what it said.

This is a false assumption.

Why? Most email archives save less than half of the transaction data. For sent email, the archives may show you what you claim to have sent, but do not prove what was actually received. Further, it is well understood that messages in your sent folder and inbox can be altered (or can be claimed to have been altered) with a few clicks of a mouse. If later disputed, your email records may not provide you with the proof and coverage you had thought you had.

In case you are curious about how easy it is to change an email record, here are some common methods:

a. Altering Timestamps: To make an email appear in the recipient's folder in a different time order, or to change the timestamp on your copy pushed into your sent folder, you can simply temporarily change the clock on your personal computer, and then send the message from commonly used email programs like Microsoft Outlook. Magically, it will appear to have been sent at that time – the timestamps on the email, the chronological placement in your sent folder, and the chronological placement in the recipient inbox will be altered. This could be used, for example, to back-date an email if a deadline had been missed.

b. Changing Message Content: In commonly used email programs like Microsoft Outlook, one can easily open the message, in the toolbar ribbon, click "Actions" and then "Edit Message", then change the text, save, and close. The email will forever be changed in your inbox or sent folder, with changes virtually undetectable. If the email is later printed to paper or PDF, you will not be able to determine what the authentic original once said. If you suspect someone else altered an email and purported it to be fact, you can point out how easy it is to change an email, and suggest that they find a way to authenticate their record.

c. Unreliable Outlook Read Receipt: Common email program read receipts have little value as they are simple text files that can have the timestamps or message content easily forged using methods noted above, and further, they tell nothing about what the original message actually said (or what was attached). Further, they are unreliable since the recipient can opt not to have the receipt returned with a simple email account setting. Generally, for external recipients (outside of your company or network) these "Outlook" read receipts are not returned. The same holds for other standard read receipt programs in Gmail and AOL, for example. Note, sending to people within your company may return more of these, but that would only be due to IT administrator settings inside your company.

Link-retrieval Systems

Some people send (or advise clients to send) disclosure documents using a link-retrieval system. The recipient receives a link to download the document. A record of the delivery of the disclosure document generally would protect the sender in certain future disputes about what risks or transaction details were disclosed at the time of entering into the transaction (think TRID real estate disclosures, financing memorandum risk section disclosures, insurance coverage terms, etc.).

Would a timestamped record showing when the document was downloaded from the link-retrieval system serve as proof of delivery of the disclosure document?

It may. But what if there is a dispute later? When it counts, the link-retrieval download record may not stand up to scrutiny as it likely would not prove what content was in fact downloaded (and received), and it likely would not prove the download was completed successfully.

How can one reliably prove fact of sufficient e-delivery of a disclosure?

First, consider what information should be disclosed. What is considered important for audit or compliance proof is the ability to irrefutably demonstrate the precise content that was disclosed.

Second, to prove that the disclosure was clear, one should be able to re-construct the original disclosure in form and format, to demonstrate how the information was originally displayed.

Third, to demonstrate that the disclosure was accessible to the recipient, it may be important to be able to show how the information was delivered to the intended recipient. For example, if the disclosure was attached to an email in a standard PDF or inserted as body text in the email, and delivered to the recipient's inbox, this would mean the information was accessible.

Fourth, the record that is relied on as proof of the above – the original content, the content inside its original context, and accessibility of the content to the intended recipient — should be in a form that is verifiable, durable, self-contained, court-admissible, and timestamped. The Uniform Electronic Transactions Act (UETA) provides a useful definition of what constitutes the time of a 'legally received electronic message' within UETA (sections 15(b) and (e)):

> 15 (b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when: (1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and (2) it is in a form capable of being processed by that system.

> 15 (e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

Similar to when mail is sent, the recipient is deemed to have "received" the email (regardless of whether the recipient retrieves the email), when it enters the recipient's "information processing system" or server that the recipient uses to receive email.

When you need visibility of delivery, assurance or proof, or simply peace of mind, you should use an email tracking service that returns irrefutable proof while preserving the simplicity of standard email — and does not require recipients to click links, register for an account, or download software. RPost's RMail service is one service that provides this level of proof and accountability for email users.

DOES THE NEW ERA OF MEGA-LEAKS OBSOLETE ATTORNEY-CLIENT PRIVILEGE?

In April of 2016, more than a hundred media outlets around the world, coordinated by the Washington, DC-based International Consortium of Investigative Journalists ("ICIJ"), released stories on the "Panama Papers", which is an exposé of private client and internal work product emails and other files. More than 5 million emails and files were stolen from within the IT systems of the exclusive Panamanian law firm Mossack Fonseca. World leaders and U.S. business people have become targets as a result of the exposed data.

There is no doubt, from reading the whirlwind of press on the "Panama Papers", that the majority of this correspondence would not have been admissible in civil court actions due to being protected as attorney-client privilege or attorney work product privilege. It is also likely that the person who provided the trove of data to the press violated a corporate non-disclosure agreement or committed an Internet crime.

But in today's environment of massive and immediate dissemination and worldwide (Internet) publication of exposed confidential information, does that really matter? If one can point to public release of the information, does that circumvent attorney-client and work product privilege? One might argue (and we will likely see these arguments more often) that in the new era of published leaks, attorney-client privilege is becoming obsolete — at least if all the correspondents do is add an "old fashioned" signature line to one's email, or a subject line phrase that makes the statement that the plain text email correspondence (think written and mailed electronic postcard) has information so sensitive that the parties intended the information to remain private and protected.

With the "Panama Papers", an anonymous "whistleblower" was able to secretly send journalists the massive set of emails and files which were then circulated to more than 400 reporters in secret over more than a year, before a coordinated effort to go public, according to ICIJ. The whistleblower and the ICIJ that coordinated the effort took great care to use encryption to mask their correspondence, according to Wired Magazine. It is unfortunate for the Mossack Fonseca law firm clients that neither the firm nor the clients appear to have been so careful.

Who might the whistleblower have been?

Perhaps this was a hacker that gained access to the firm's IT systems. Or, perhaps this was a disgruntled IT staffer, consultant, or outsourcer that copied the database of files before leaving the firm, and then sold it to some third party. How much did they sell it for? $10,000? $100,000? $1 million? Whatever the price, the reputational damage to Panamanian law firm Mossack Fonseca and its clients is far greater.

In these scenarios, it is important to remember that plain text email correspondence can be exposed in route in many ways, and certainly on a company's mail servers, anyone with access can read these messages at will.

Let's assume IT staffers are loyal and committed to using best efforts to protect their employees and employers, and as such, they often go the extra step of

setting up encryption at the mail gateway – – so everything leaving the firm is encrypted when it hits the Internet. We know, however, that they often cannot control what happens to your message upon receipt at the recipient destination, and often it is out of their control if email archives store messages and attached files unencrypted and are somehow accessed by an unauthorized person. The "whistleblower" treasure trove, as we may find out from Mossack Fonseca, may have been the email archive (in house or outsourced) database containing the unencrypted messages before sent at the mail server (before reaching the Internet) and after received (from senders by the mail server and perhaps decrypted by the mail server).

Whatever the source, the important learning is to consider what might one do when one needs to communicate with one's client or among staff with sensitive client matters? We suggest trust no one, and use "Outbox-to-Inbox" email encryption rather than "network-level" or "policy-based gateway" encryption, if your information is sensitive to the highest degree.

RMail encryption calls this "Outbox-to-Inbox" email encryption "Executive Mode" encryption and recommends use for those dealing in merger, acquisition, corporate litigation strategy, private client wealth management, and personal health matters; matters that one would like to shield from their IT staff or the IT staff at the recipient.

RMail Executive Mode encryption encrypts the message locally in the sender's Microsoft Outlook program at the sender's desktop or device, and ensures encrypted delivery straight through to the recipient's desktop; securing from the potential of data breaches both within the sender's in-house or outsourced email system, and external while in transport across the Internet and within the recipient's email system. This also provides for letting the recipient encrypt replies without having RMail at their end.

With RMail Executive Mode encryption, the message and all attachments remain encrypted within the recipient's email inbox, and are printed and encapsulated inside a PDF file, readable after decrypting in one's PDF reader (outside of the inbox) and if saved, remain saved in encrypted file format unless the recipient extracts the attachments and chooses to use them as normal files. This end-to-end encryption uses a 256-bit AES encrypted PDF wrapper to keep one's message and any attachments private from start (while sitting in outbox) to finish (even while sitting within their inbox), so only one's recipient can read them.

There are other ways to do something similar, using PKI or PGP encryption, but in each of these methods, depending on how deployed, the message is decrypted in the recipient's inbox and remains so, are usually too complicated for normal senders and normal recipients to use, or requires special software at the recipient end which introduces more complexity.

Would RMail Executive Mode encryption have protected Mossack Fonseca clients from this mega leak? It may have. It certainly should have at least been an option in the client or lawyer toolkit to protect information in this new era of mega leaks.

UNDERSTANDING DATA PRIVACY COMPLIANCE: ENFORCEMENT, ENCRYPTION, AND AUDITABLE PROOF

Email encryption is one of the strongest defenses that an organization can implement against data breaches brought on by the improper disclosure or distribution of personal financial and non-public consumer information; in particular if one is communicating on behalf of their client.

For investors, it is really your responsibility to choose service providers that are comfortable using tools like email encryption to protect your sensitive information. Ask your professional service providers (lawyers, bankers, brokers, realtors, investment advisors, investment retirement custodians, asset protection and trust specialists, corporate administrators, tax professionals, among others) to communicate with you encrypted -- if it is too challenging for them to do so, or if they use a system that is too cumbersome for you as a recipient, you might consider whether that service provider is the right one for you.

For professional service providers, it is your requirement (often regulatory requirement) to protect your client's information. You really must have a sim-

ple-to-use method of communicating with email encryption, certified e-delivery, secure e-signatures, and secure file transfer tools.

Non-compliance is not an option with today's heightened regulatory agenda.

One issue that we have seen is that even though organizations have email encryption, these systems are often cumbersome to use at the recipient side (requiring account registrations, logins, downloads, etc.) and people then don't use them. By contrast, RMail email encryption has been top rated due to its security, auditable proof of compliance, and simple user experience at the sender and recipient.

An effective compliance solution is one that can accommodate the full extent of consumer data protection regulations and control the privacy, security, and integrity of client communications. There are dozens of compliance solutions on the market today, but few that allow users to achieve compliance, illustrate full documentation, and with a record of compliance to protect in case of a regulatory or other compliance audit.

CURRENT TRENDS IN COMPUTING POWER AND ENCRYPTION

The importance of secure communication has never been greater as increasing amounts of vital business and personal data are daily transmitted by electronic means. Encryption is the core of secure communication but the cryptographic techniques most widely relied upon today may soon be rendered obsolete by technological advances. Most of those techniques rely on the fact that some mathematical operations that are so computationally difficult as to render cryptanalysis a practical impossibility. But how computationally difficult an operation may depend upon the power of computers available and it is generally anticipated that the advent of quantum computing will make it possible to execute many cryptographic calculations in much shorter time periods, rendering existing ciphers breakable in practice. When the practical applications of quantum computers are discussed, code breaking is typically among the first mentioned.

Quantum cryptography is sometimes held out as the antidote to quantum code-breaking. The hope is that the phenomenon of quantum entanglement can

be used to eliminate the possibility of third party eavesdropping. The problem is that while quantum computing is proceeding to practical reality very quickly, progress in the long distance, reliable entanglement required for quantum cryptography is proceeding very slowly. Moreover, even when Quantum cryptography is ready for practical use, deploying the technology will likely require a massive new communication infrastructure. So, while the first quantum computers have already sold commercially, the prospects for practical quantum cryptography seem remote.

It is possible then that we are fast approaching what might be called a "cryptographic cliff". A tipping point when, suddenly, no existing cipher method is reliably secure; a time when all the cryptographic walls we count on to protect us, come tumbling down. Private individuals will be left especially vulnerable to the early adopters of quantum computing who will likely be governments and large corporations.

Some are confident that quantum computing is becoming or will soon become a reality. Quantum computing will make extra-ordinary computing power available to the mass market. It is believed by some that this will trigger the collapse of the cryptographic infrastructure underling the internet – encryption based on patterns or mathematical algorithms. Why? These will be able to be deciphered with then common computing power, regardless of the patter/algorithm complexity.

The new problem, then, is quantum computing will render imperfect (pattern based) encryption obsolete, and trigger the collapse of the cryptographic infrastructure that underlies internet communications.

The new standard for encryption therefore, must be perfect -- unbreakable in principle -- encryption.

Further, given recent revelations about the NSA's capacities and given the imminent prospect of quantum computing, any method of encryption which is less than perfect cannot be relied upon now or at least in the near future. The only safe course is to assume that any encryption code that is breakable in principle has been or can be broken in practice. This is not going to get better, ever.

We believe that in the near future all genuinely secret communications will incorporate some form of One Time Pad method of cryptography – encrypting messages using unique sets of random data, each set only used once. In one sense OTP is an old fashioned solution to a new problem.

We believe that in the near future all genuinely secret communications will incorporate some form of One Time Pad method of cryptography. The new standard for encryption will need to be perfect.

The traditional challenge with One-Time-Pad methods of cryptography for communications is that each person that one communicates with must have a unique set of random numbers shared only with the recipient of that message, to be used to determine the "shift" in letters; then never using that set of numbers again to "shift" letters in a future message; and permanently shred the numbers so that they can never be used to decipher a past message. And, this must be done in a unique way for each sender – recipient pair; and further, each message intended to be read my multiple recipients must be uniquely transmitted with the shared "shift" numbers with each intended recipient… and then how does one secure all of these pads and keep track?

However, if these challenges can be overcome, those seeking perfect secrecy in messaging may have a way, as randomness rules. Random data cannot be deciphered regardless of the computing power of the eavesdropper.

Where to Find the Tools?

Tools discussed in this Guide include:

1. Microsoft Office®, Microsoft Office 365®, Windows 10. These are available from Microsoft® corporation. (Microsoft.com)
2. Gmail, available from Google®. (Gmail.com)
3. RMail® email security services, available from RPost® (Rmail.com)

ABOUT THE AUTHOR

Zafar Khan is CEO of RPost Communications and a frequent faculty speaker on cyber security and compliance for national industry associations. RPost is the global leader in secure and certified electronic communications and World Mail Award winner for "Best in Security." RPost has helped businesses enhance their security, compliance, and productivity for more than a decade with services to track, prove, e-sign, encrypt, and secure, used by more than 25 million people throughout the world.

Khan holds a Bachelor's degree from Wesleyan University, an International Business Certificate from The Georgetown University School of Business, and an MBA from The Wharton School at the University of Pennsylvania. Khan has participated in a Presidential Trade Mission led by the US Secretary of Commerce and has been designated one of the top 100 technology CEOs. Khan previously worked for Goldman Sachs in New York and Deloitte Consulting in Los Angeles.