EY
Building a better working world

Cybersecurity: protecting a family office

By Charlie J. Carr, CFP®

Contents:

Introduction

Cybersecurity is a hot topic among family offices, and for good reason. The American Institute of Certified Public Accountants (AICPA) reported in 2015 that 25% of Americans have been victims of information security breaches in the last year, which is double the rate of the prior year[1]. Verizon reported in 2012 that 71% of cyber attacks occur at firms with fewer than 100 employees,[2] while the National Cyber Security Alliance states that small businesses that get hacked have a 60% chance of going out of business within six months[3].

Most people admit to being concerned about cybersecurity, but at the same time, do not understand it or know what they should do about it.

Wealthy families have always been ripe targets for thieves and vandals, and the rise of the internet and electronic tools opened additional avenues for such criminals to operate — often with a cloak of anonymity. FireEye reports that only 10% of cyber crimes reported to police actually result in a conviction[4]. The crimes identified in recent headlines are disconcerting:

- *IRS says thieves stole tax info from 100,000 households (Fox News, 5/27/2015)*[5]
- *Hackers raid eBay in historic breach, access 145M records (Reuters, 5/22/2015)*[6]
- *Home Depot hackers used vendor log-on to steal data, emails (USA Today, 11/7/2014)*[7]
- *Hacks of OPM databases compromised 22.1 million people (Washington Post, 7/9/2015)*[8]
- *Saks Fifth Avenue employees busted in identity theft ring (NY Daily News, 10/6/2014)*[9]

The issue is serious, the threats are confusing, and advice for dealing with the threats is often unrealistic. Ask a technologist which criteria should be used for passwords, and you are likely to hear something similar to this:

> *Use a unique, 16-character password for every site and tool; do not use any known words in the password; include a mix of uppercase and lowercase letters, numbers, and special characters; never write it down; and change the password every 30 to 90 days.*

Considering that many of us have 25 or more such passwords, we are not able to follow these stringent guidelines. This paper explains the cyber security challenge for family offices, describes the most common risks they face, and offers a measured approach to address the challenges.

Define the risks

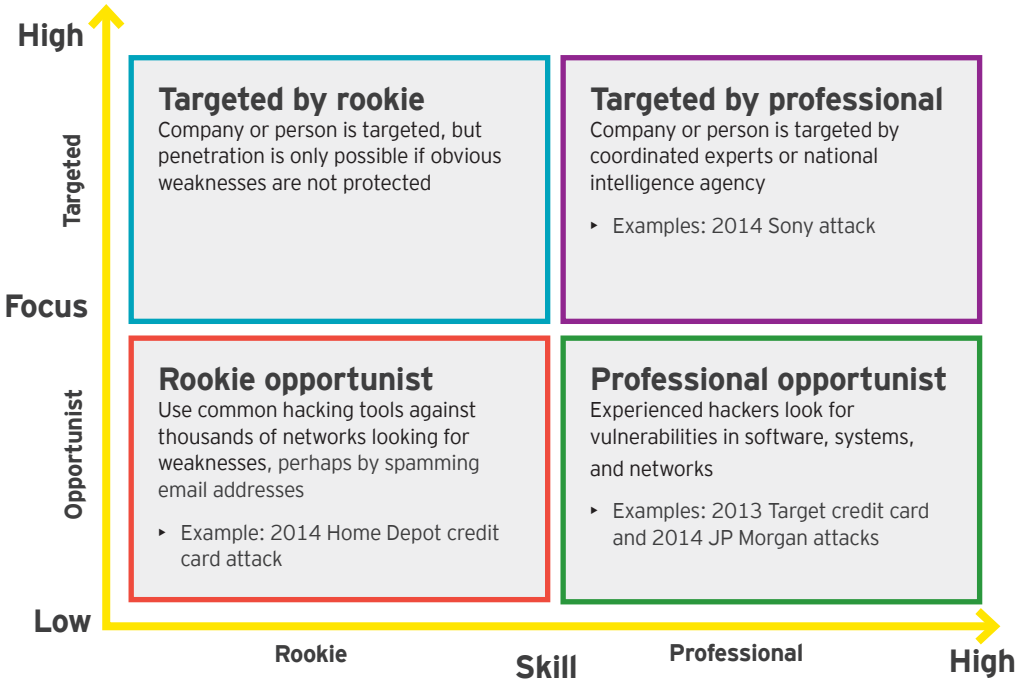
Family members often are on the leading edge (perhaps bleeding edge) of new tools and technology, and sometimes believe they are impervious to technology risks. One family member told us the family office's network security was too onerous, so she just goes to the coffee shop to use Wi-Fi. She didn't realize that doing so risks not only her own privacy, but also that of the entire family and family office.

A common mantra is, "there are two types of companies: those who have been hacked, and those who don't realize they've been hacked." Families are similarly at risk.

The nearby chart maps hackers based on skill level and focus (opportunists are looking for "unlocked doors"). Basic security measures (outlined later in this paper) protect a family from three of the four boxes – all except the top right corner. Fortunately, most hackers fit into one of these three boxes. However, industry experts say that adept hackers can get into nearly any system. If a family is targeted by highly skilled hackers, perhaps even state-sponsored hackers, the best they can do is make it hard for them to get in, and through monitoring, identify intrusions quickly and limit damage by shutting the systems down.

Why should a family be concerned about potential cyber intrusions? At its core, there are three key concerns:

1. **Theft.** Someone might access bank, credit, investment or other financial accounts. Even if the family refuses to use online banking, their money may be at risk through phishing attacks, automatic teller machine (ATM) fraud or someone accessing their information at the IRS.
2. **Privacy.** Hackers may harm the family reputation (or its business) by revealing details about the family wealth, while thieves may use information to plan a robbery or kidnapping.
3. **Maliciousness.** Just as teenagers might spray-paint graffiti on a building, hackers may access data or websites just to delete or destroy data, or perhaps to redirect users to a different website. This may cost the family privacy, in addition to the cost of repairing the websites.



Threats by mode

We can put threats in three categories to help identify and understand them.

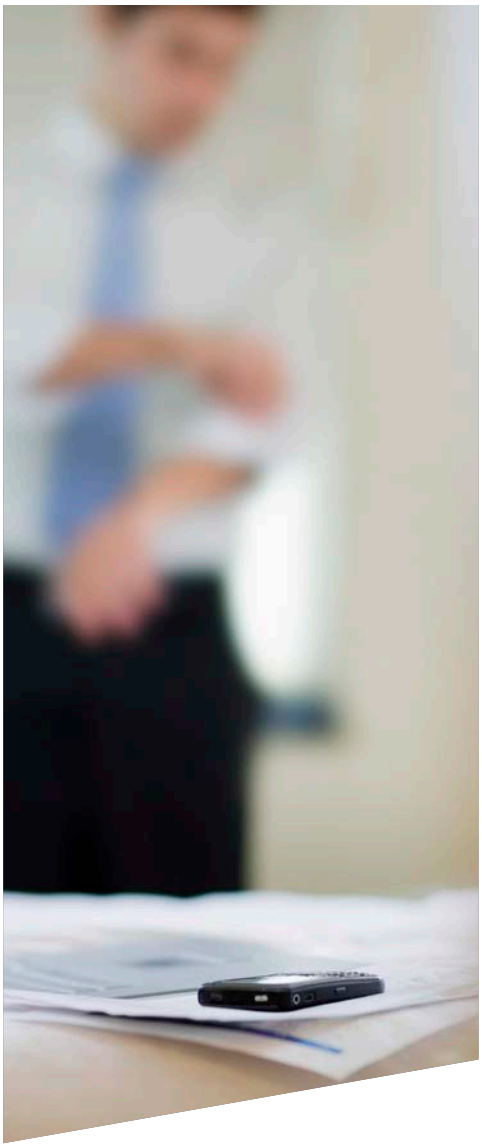
Devices

- Many of us have become accustomed to computer viruses and similar attacks. Any desktop or laptop computer (not just Windows-based machines) is vulnerable to such attacks.
- Mobile devices, such as smartphones and tablets, also are vulnerable to attack. Any contacts or personal information on the device may be accessed, and if the device is used to access the internet via unsecured Wi-Fi, passwords and other information may be at risk.

  It's worth exploring mobile devices a little further, since most of us have smartphones. Verizon's research looked closely at mobile devices, and discovered that only 0.03% of mobile devices were infected by higher-grade malicious code – a negligible portion. This excludes low-grade malware, which is mostly annoying pop-up advertisements. FireEye reports that 96% of mobile malware targets Android devices rather than Apple devices[10].

  Does this mean that we don't have to concern ourselves with cyber security on our smartphones? It means we have fewer concerns with the security of the device itself, but we still have to be concerned with what we do on the device. Even if your smartphone is not infected, if you are using unsecured Wi-Fi at your local coffee shop to log into your online bank, you may have just exposed your bank password.
- Any device with online access is vulnerable, including connected devices in a smart home. Some risks that may not immediately come to mind are a nanny-cam that can be accessed through the internet, door locks that can be opened with a smartphone, vehicles with built-in Wi-Fi, and air conditioners and other appliances that can be controlled online. In 2015, two computer-security researchers showed that they could hack into a Jeep Cherokee, controlling the vehicle's software and its speed using a laptop miles away[11].

Verizon conducts annual research into data breaches, and showed that more than 99% of 2014 hacks exploited a vulnerability that had been identified and patched more than one year previously[12]. In other words, if users had updated their software in the prior year, they would not have been exploited.



Cloud

Any business or family website is vulnerable to attack, either to capture information (e.g., steal credit card authorization data), to reveal private information or for malicious behavior (e.g., delete and replace content). Many families have a cloud-based document storage tool, through a private family website or through a third-party provider, to allow family members and advisors to access shared documents. Such families also may use internet-based accounting systems.

Most banks, credit cards and investment firms provide data access via the internet. While such firms often are the most diligent to protect their clients' security, they still represent a point of vulnerability to the family, particularly if the family accesses such sites through insecure methods or uses easily guessable passwords.

Many families refuse to use cloud-based software or tools, based on the risk of someone hacking into the data. However, that may put them at greater risk of losing their data if there were a fire or disaster in the office. In addition, there may be more robust and efficient tools that are only available in the cloud. Most families want to balance their security with the capabilities and services that are available in the cloud.

Access points

Families access the internet through many different channels, in addition to accessing family office files remotely over the internet. Each of these access points represents some risk.

- An often-overlooked vulnerability is home and office routers (used for Wi-Fi around a house) and the passwords used for accessing them. Thieves may drive around a neighborhood, trolling for unsecured Wi-Fi networks. Families often think that what they do in their own home is secure, but that is not true if someone gets into their Wi-Fi.
- Public Wi-Fi, perhaps at a hotel, airport or coffee shop, while a nice convenience, also is a serious risk. Thieves can be online in another room at the same hotel, stealing passwords and private information from unsuspecting users.
- Passwords are always a point of risk, whether to an email account, online banking or various websites. The more complex the password, the more likely someone is to write it down. We've seen family offices where every staff member had a copy of a password sheet with the various online banking and other account passwords. The cleaning people could easily copy the sheets each night, giving them full access to financial accounts.

There are some cyber threats that do not fit cleanly into any of the three categories, so we'll explore them here.

- **Phishing** is a method of defrauding someone by posing as a legitimate person or business. Most commonly, this involves sending emails to get recipients to log into a website and provide password or other confidential information. It might appear to be an email from your bank, or a package delivery company, with a link suggesting there has been fraud involving your account. Following the link may result in real fraud occurring, as you now provide the person your real login and password information. Several years ago, these emails were more obvious as the spelling and language were poor, obviously written by someone not native to the US. However, they have improved significantly in recent years.

  Several family offices have reported an insidious form of these attacks. Someone hacks into a family member's email account. Often, he or she monitors the account for a period of time to see the language used and types of emails sent. Then, the hacker sends an email to the family office, mimicking the member's style and requesting that a wire be sent. If the family office isn't diligent on its payment protocols, the wires are sent as instructed and the money is lost.

  Verizon reports that more than two-thirds of the nearly 80,000 security incidents that it studied in 2014 featured phishing. Its research shows that 23% of recipients open phishing messages, while 11% click on the attachments[10].

  These scams can be done on the phone as well. The Federal Trade Commission (FTC) reports a 24-fold increase in complaints in 2014 from consumers who received a call from someone pretending to be an IRS official. The caller tells the consumer he or she owes tax penalties, and tries to get him or her to wire money or load money on a prepaid debit card[13].

- **Debit and credit card fraud** has received quite a bit of attention recently. Some firms have discovered devices attached to an ATM, reading the card when inserted. Users receive cash as usual, but thieves now have their account information and password. *The Wall Street Journal* reports that in the first three months of 2015, such attacks reached the highest level in at least 20 years[14]. In other cases, waiters or store clerks have stolen account information. Fortunately, consumers have limited, and often zero, liability for such fraud, as long as they report the crime timely. They still have a hassle with getting new cards and accounts, but they usually do not lose money.

10-point family office cyber protection plan

With so many risks, and knowing that most wealthy family members have very little patience for security and restrictions, we have developed a 10-point plan that family offices can use to protect the family's technology. This plan is designed to be reasonable for the family, while limiting their exposure to the most common threats. Some high-profile families may choose to exceed these recommendations.

1. Technology inventory

The family office should maintain an inventory of routers (don't forget those at each family member's house), computers, tablets, phones and other devices. The office needs to maintain these devices and make sure that each one has updated antivirus, firewall and similar software.

As part of the maintenance, the office should ensure that software on the systems, such as operating systems, Microsoft Office, browsers, and accounting tools, is kept current.

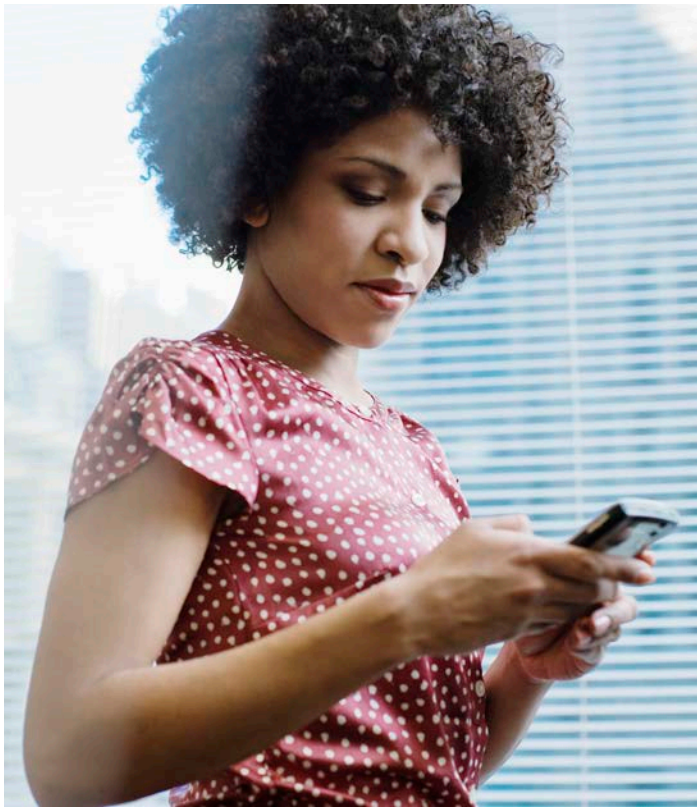
The inventory also should track email accounts held by the family, with an understanding of how they are used. If the accounts are used for sensitive or private matters, it may be necessary to use secure or encrypted email, or perhaps to suggest other means for communicating.

In addition, the inventory should track databases and the types of data contained therein. Most important are databases with client information, but also anything that thieves can exploit.

2. Written cyber policy

Family offices should have a written cyber-protection policy, including a connected-device policy, a password policy, social-media policy and payment-authorization policy. Families rarely have penalties for violating these policies, but by writing them down, communicating them and providing education, the family understands and thinks about their behavior.

- The connected-device policy describes where and how the family wants family members to connect to the internet. Some families ban the use of public Wi-Fi, requiring that members use the data plan on their cell phones instead. Other families permit the use of public Wi-Fi, but require use of virtual private network (VPN) tools to protect privacy. Some families set a policy that home routers are non-discoverable, or such that someone cannot see the Wi-Fi in a list of available connections. Instead, they would have to enter the name of the Wi-Fi and then the password.



- A password policy describes what the family believes is a reasonable standard for different passwords. These policies often address types of sites that should have unique passwords versus those where someone might re-use passwords. Some family offices pay for family members to use password utilities to manage and simplify password use.
- Social-media policies address how family members use social-media tools, and what types of data can be shared outside the family. The concerns are sharing information that might put personal security at risk, that reveals private details about family wealth, or that can hurt the reputation of the family or the businesses.
- Payment-authorization policies mimic what a bank might do to approve wires or other payments. There are numerous examples of family member emails being hacked into, and offices making payments based on fraudulent emails, purportedly from the family member. Such policies are not aimed at controlling family spending, but rather at ensuring that payments made are authorized and proper.

3. Cyber security insurance policy

If the family office oversees family businesses, blog sites or foundations with websites, they should consider cyber security insurance. Such policies can cover:

- Liability for loss of data, such as client personal data or credit card details
- Remediation costs, such as investigation, notification and repairs
- Settlement costs, such as client-monitoring services, payments or regulatory fines

Cyber insurance typically gives the family office access to the right experts in times of crisis to help identify and resolve the problems.

4. Vulnerability assessment

Vulnerability assessments identify the weaknesses in a system. For a family office, this should include the family office, businesses overseen by the office (including a foundation office) and each family member's home systems. Most offices lack the expertise to conduct these assessments internally, and thus contract with an outside vendor. Such assessments should be conducted at least annually.

Penetration testing (often called Pen Testing) uses "ethical hacking" to simulate what a cyber attacker might do by attempting to penetrate the system. It essentially addresses whether someone can break into the system, and if so, what they might steal. This is more costly than vulnerability assessments, and the office should consider its own risk and the importance of the data when deciding if this is necessary. Many businesses conduct Pen Testing annually or ongoing basis, while most family offices do not conduct such testing or only do so every few years.

Ethical phishing attacks (e.g., sending emails to staff and family members, trying to get them to access suspect websites or to provide private information) are a form of Pen Testing and should be seriously considered for every family office. Most offices prefer using an outside firm for these attacks.

5. Encryption tools

Most offices find it necessary to share confidential information electronically with family members and outside advisors. This may entail sending social security and transaction information to the family's tax accountant, providing balance sheet and performance data to family members, or having strategic business acquisition discussions with family or advisors.

If sent in standard emails, the data passes through the internet and could be intercepted and read by hackers. One way to prevent this is to use email encryption tools. These tools encode the message before it is sent, and the receiver has a similar tool to decrypt and read the secure message. If someone intercepts the message, it will be indecipherable unless they have the proper decryption tool.

Another way to accomplish this is to use a secure, cloud-based document storage tool. Rather than emailing the file, the family can copy the file to a folder in the tool and give the advisor access to the individual file (or perhaps to the entire folder). Obviously, the family will want to be comfortable that the document storage provider is adequately securing the data.

6. Identity protection

Despite all of the best efforts, there remains a risk that a family member's identity could be stolen. This may be by a clerk at a restaurant or department store where the member used a credit card, or perhaps the family member was one of the more than 100,000 people whose information was hacked on the IRS website[5]. Maybe the family member was targeted by professional thieves based on a magazine article or other public information.

There are many firms that will monitor any new account openings, credit requests and similar activity. They notify clients of any activity, giving them the opportunity to validate the request and prohibit transactions, if desired. They also can create a freeze, such that new accounts cannot be opened. If someone's identity is stolen, these firms are experienced in helping the person recover from such theft. Many family offices provide such services for each family member.

7. Cyber education

The family office can use the most robust tools and vendors available, but they need to be paired with education on the risks for family office staff and family members. Family members need to understand how their social media posts may cause harm, how thieves may use phishing techniques to obtain passwords or other key information, and how hackers obtain email passwords and use family member emails to request wire transfers. Cyber education should be a key part of annual family meetings to help family members understand why the family technology policies were created, and what can happen if they are not followed.

Don't neglect the younger generations in this training. Most likely, preteens, teenagers and those in their 20s are the most technology-savvy in the family. They also may be the least concerned with family privacy, and may use their technology skills to turn off firewalls and avoid security. Their comfort with technology could become the family's greatest threat[15]. The answer may be in education — helping them realize the risks to the family. The best tools might be real examples of what has happened with other families or businesses.

8. Data backups

Few people have the discipline to consistently back up their devices on their own, making it a key function for the family office to address. While backups can be done on thumb drives or external hard drives, it is generally preferable for backups to be stored off-site, which frequently requires a cloud-based provider. On-site backups could be lost if there is flood, fire or other disaster at the office. The office should research backup providers carefully to ensure security is not compromised.

The office should automate the backups to the extent possible, so the family does not have to launch or initiate the effort. If a device is lost or stolen, or if a hacker destroys data on a device, the family can restore the data from a backup version.

9. Background checks

The family office should conduct criminal background checks annually on family office staff and vendors. Many offices conduct such checks before hiring staff, but then never do so again. If an employee is with the family for 10 or 15 years, the office may not be aware of subsequent arrests. When using a vendor firm (including technology providers, consultants and household staff), the firm itself may perform background checks on the staff, which may be sufficient. The office should seek proof of such checks, and if not performed, then do so themselves.

In EY's 2014 Global Information Security Survey, 57% of respondents said that the most likely source of a cyber attack is an employee, and 35% said it was a contractor working in their offices[16]. *The Wall Street Journal* reported in April 2015 that somewhere between 20% and 67% of data breaches involved hackers gaining access through a vendor or third party[17]. Target, Home Depot and Goodwill Industries

all traced recent large data breaches to outsiders with access to their networks.

10. Network monitoring

Family offices should have staff or a vendor monitoring the family office network, business networks and family home networks, looking for signs of an intrusion. Very few family offices have the proper staff to do this internally, so they should rely on trusted outside firms. Such firms monitor systems 24 hours a day and can shut them down in the event of an attack.

Password practices

Online searches indicate that the average person has between 19 and 40 online passwords. Families often ask what policies they should follow and how they can track the different passwords. The answer provided at the top of this paper is the safest one; but as indicated previously, it is not realistic for most of us.

We'll start with definitions. Websites require authentication to verify that the user is authorized before allowing him or her to see private or personalized information. Such authentication can involve something known (a password), something possessed (such as a smart card) or part of their body (voice or fingerprint). Single-factor authentication uses one of these items, while two-factor authentication requires two of these items. It is harder for someone to steal both the password and the smart card, making dual authentication more secure.

A 2013 Ofcom (UK communications regulator) study showed that 55% of adults used the same password for most websites[18]. If one site gets hacked, the hacker now has the user's password for other sites. This is certainly not a best practice.

If 16-digit passwords, different for each site and never written down, are not realistic, then what is? We must balance security and memorability — longer, more complex passwords are harder to guess or hack, but they're also harder to remember. In such cases, users are more likely to store them insecurely and expose them to attackers. It's important to balance desire for password length and complexity with the practical reality of how users will implement the requirements.

The nearby policies (dos and don'ts) may not seem to simplify this process, but here are some additional suggestions to make this more practical:

- Some easy-to-remember passwords are collections of words that form a phrase or sentence — perhaps the opening sentence to your favorite novel or the opening line to a good joke. "It was the best of times; it was the worst of times" could be "IwtbotIwtwot" (first letter from each word). Perhaps even use a "0" instead of an "o", or a "1" instead of an "i".
- Another suggestion is to use a goal for your core password, and add characters for the specific site (perhaps "Lose10lbsAA" or "AAgo2hawaii" for your American Airlines password). Each time you enter the password, you reinforce the goal — and accomplishing the goal may prod you to change your password to something new.
- For password reset questions (e.g., "click here if you forgot password"), consider "false known" responses. For example, if it asks for your favorite color, make the response "twelve". You'll have to remember you did that, but a hacker would not be able to guess the answer. Also, don't use any questions or responses that are easily found in public spaces, such as your high school or college mascot, unless you use a false response, as described above.

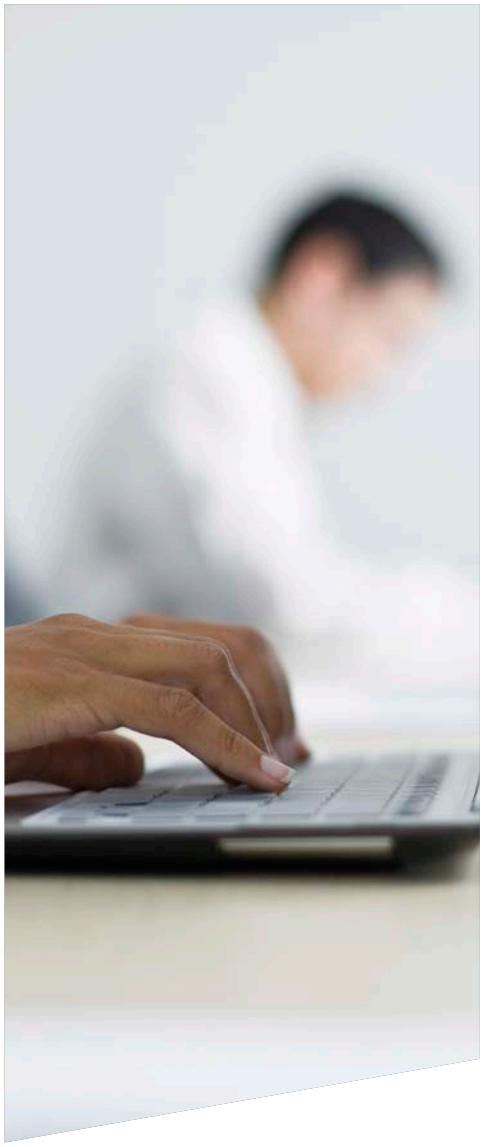
Password dos	Password don'ts
▸ Use unique passwords that combine words, numbers, symbols, and uppercase and lowercase letters.	▸ Don't use your network name or email address as your password.
▸ Use different passwords for different secure sites. For sites that do not store financial or private information, you may consider a common password.	▸ Don't use easily guessed passwords, such as "password" or "123456".
▸ Change passwords regularly, even if the site doesn't require it. Changing every 60 days is ideal, but even a semiannual or annual change is better than what most people do.	▸ Don't choose passwords based on personal details, such as birthdates or family names.
▸ If you must write down a password, write just a clue or abbreviated form — something that only you can decipher. However, still don't leave the clue in obvious or easily found places.	▸ Don't use dictionary words or names in their correct form.
▸ While 12–15-character passwords are ideal, it is best to use at least 8 characters.	▸ Don't use the same password at multiple secure sites. Consider a common theme with unique twists.
▸ Consider a password utility service.	▸ Don't share your password online or over the phone — not even with friends or family.
	▸ Don't enter passwords to secure sites while using unsecure public networks, unless you are using a VPN.

Appendix A — Glossary

1.	**Antivirus software**	software used to prevent, detect and remove malicious software
2.	**Cloud**	general term indicating data stored or services delivered over the internet
3.	**Cyber attack**	attempt by hackers to access, damage or destroy a computer network
4.	**Denial of service attacks**	attempt to make a server or website unavailable to users. This usually involves code that floods or overwhelms the system.
5.	**Dual factor authentication**	requires two steps to access a site. This might be a password plus a card key
6.	**Firewall**	digital perimeter that keeps out viruses, thieves and hackers
7.	**Hack**	gain unauthorized access to a computer or system
8.	**Identity theft**	fraudulently using someone's private, identifying information
9.	**Malware**	software designed to damage or disable electronic devices
10.	**Phishing**	posing as a legitimate company or person to defraud someone electronically
11.	**Secondary attack**	website is attacked to plant malware, in hopes that the electronic device of the person or business targeted becomes infected. The site where the hacker planted the malware was not the target, and is just a vehicle or a secondary victim.
12.	**Spam**	send irrelevant messages to a large number of people online
13.	**Virtual private network**	A VPN creates an encrypted connection over a less secure network
14.	**Wi-Fi**	facility allowing electronic devices to connect to the internet wirelessly in a given area

Appendix B — Sources

1. "AICPA Survey: One-in-four Americans victimized by information security breaches"(*AICPA press release*, 21 April 2015)
2. "Verizon 2012 Data Breach Investigations Report" (May 2012)
3. "Protecting yourself against cyberattacks" (*Pete Walkey, ARGI Financial Group*, 20 May 2015)
4. "Not Too Small to Matter: Five reasons why SMBs are a prime target for cyber attacks" (*FireEye white paper, 2015*)
5. "IRS says thieves stole tax info from 100,000 households" (*www.foxnews.com*, 27 May 2015)
6. "Hackers raid eBay in historic breach, access 145M records" (Reuters, www.cnbc.com, 22 May 2014)
7. "Home Depot hackers used vendor log-on to steal data, e-mails" (Michael Winter, USA Today, 7 November 2014)
8. "Hacks of OPM databases compromised 22.1 million people, federal authorities say" (Ellen Nakashima, The Washington Post, 9 July 2015)
9. "Saks Fifth Avenue employees busted in identity theft ring" (Edgar Sandoval, Corky Siemaszko, New York Daily News, 6 October 2014)
10. " Verizon 2015 Data Breach Investigations Report" (May 2015)
11. "Hackers show how flaw lets them control a car" (Danny Yadron and Mike Spector, *The Wall Street Journal*, 22 July 2015)
12. "Verizon research: 99.9% of hacking incidents use vulnerability that has been known for at least 1 year" (*The Wall Street Journal* article on 14 April 2015).
13. "IRS Imposters, Scams are running rampant" (*Pamela Yipp, Dallas Morning News*, 8 March 2015)
14. "Debit Card Data theft at ATMs is soaring" (Robin Sidel, *The Wall Street Journal,* 20 May 2015)
15. The Weakest Security Link: Your Children (*The Wall Street Journal,* 20 April 2015)
16. Hot Topics – Cyber Security (EY, February 2015)
17. "What Companies should be doing to protect their computer systems – but aren't"(Danny Yadron, *The Wall Street Journal*, 20 April 2015)
18. "More than 50% use the same password for everything" (Huffington Post, 23 April 2013)
19. "Fraud worries: debit vs credit cards" (*The Wall Street Journal,* 23 May 2015)
20. "What is Encryption, Anyway?" (*The Wall Street Journal*, 20 April 2015)
21. "Cyber Insurance: one element of risk management" (*The Wall Street Journal*, 18 March 2015)
22. "32 Data Breaches Larger than Sony's in the Past Year" (Kyle McCarthy, huffingtonpost.com, 8 January 2015)
23. "Millions more Americans hit by government personnel data hack" (Reuters, 9 July 2015, Patricia Zengerle and Megan Cassella)
24. "How small businesses can fend off hackers" (Lou Shipley, *The Wall Street Journal*, 17 July 2015)



About the author

Charlie Carr is an Executive Director in EY's national tax practice who focuses on advising family offices. Charlie has over 25 years of financial services experience, including more than 10 years working exclusively with family offices.

Charlie's goal is to inspire families to achieve their legacy for the next 100 years. He provides particular insights into wealthy families, their family offices, and what they want from financial services firms. He has worked with hundreds of family offices, helping families create the family office that best meets their interests and goals, including defining what services to offer, finding technology that supports those services, identifying risks in the office, and defining efficient processes to support the family.

Charlie holds a Bachelor of Business Administration in Accounting and Management from Baylor University. He is a CERTIFIED FINANCIAL PLANNER™, and has a Six Sigma green belt for process design. Charlie has been a youth baseball coach since 2001, and in 2012, he developed and taught a personal finance class for high school students. Charlie lives in Flower Mound, Texas, with his wife and 3 sons.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

1507-1577884_SW

ey.com