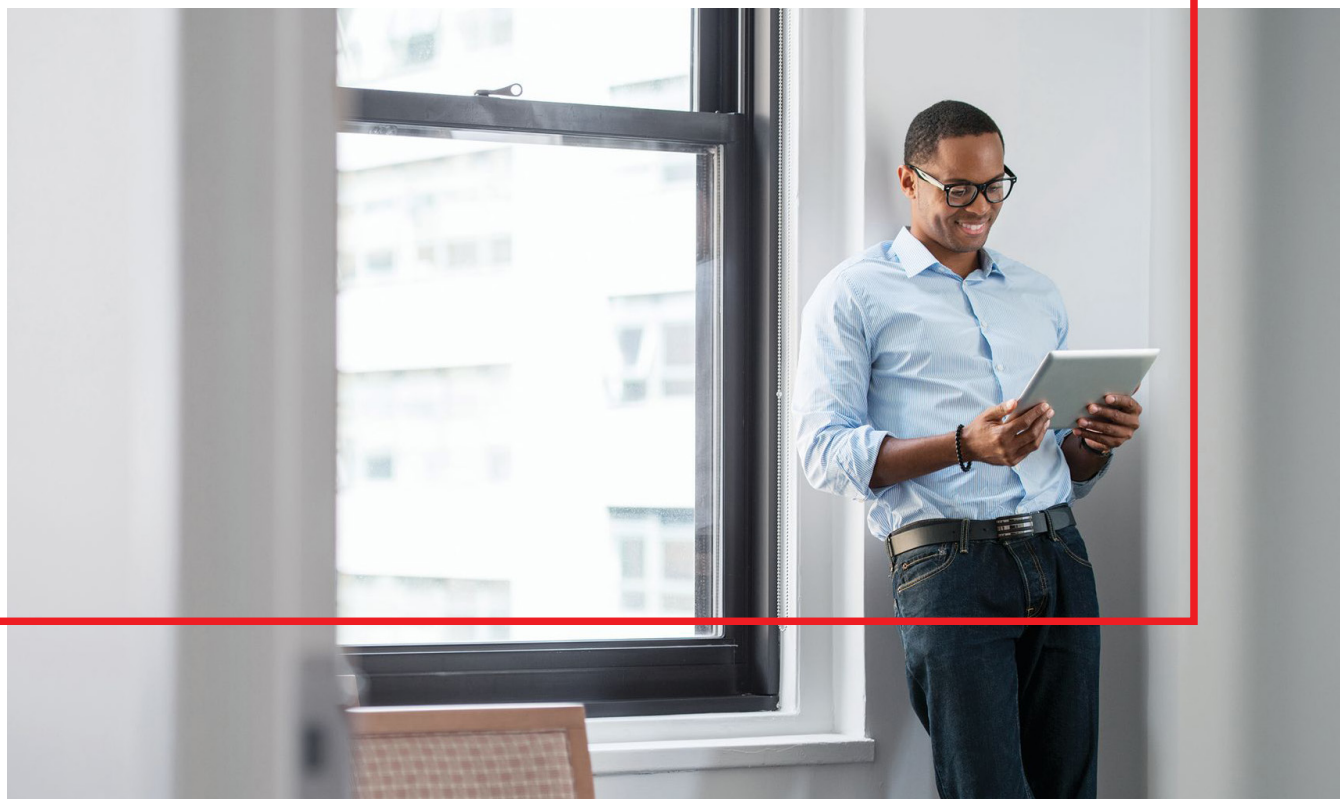
UBS

Staying cyber safe

A guide to outpacing ever-evolving cyber threats



UBS Family Office Solutions and Cyber & Information Security

Contents

Author
Sejal Pattni
Global Head of Cyber Education
& Awareness
Cyber & Information Security

Production team
Meredith Johe
Head, Business Development
Family Office Solutions

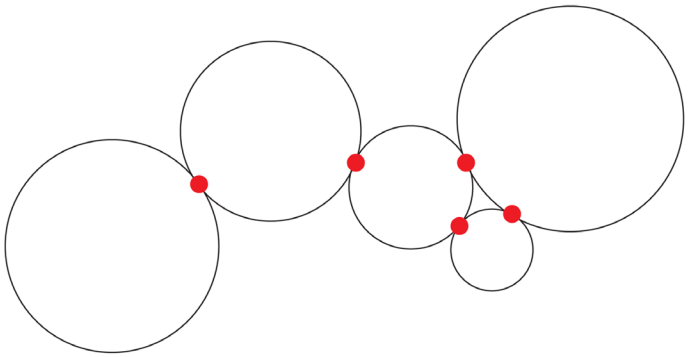
Brittany Chajkewicz
Business Analyst
Family Office Solutions

UBS centers of excellence

UBS serves high net worth and ultra high net worth individuals, families and family offices across the globe by connecting clients to expertise, advice and customized solutions—from across the firm and around the world.

Family Office Solutions is a team of specialists that exclusively works with USD 100 million+ net worth families and family offices. The team helps clients navigate the challenges and opportunities across their family enterprises, including their businesses, family offices, philanthropic structures, and passions and interests. Having this expertise under one roof allows for integration and layering of services across the UBS ecosystem, delivering a personalized, holistic client experience.

Cyber & Information Security (CIS) manages cyber and information security risks. The team covers cyber threat management and defense to proactively understand, detect and respond to threats, and cyber risk management to set priorities and prevent threats. The number one priority of the team is our clients and the safety of their assets and data.



Why be cyber safe

Cyber threats worldwide have evolved in both volume and sophistication as espionage, data theft and attempts to disrupt day-to-day services have spread into the digital world. As our dependency on digital tools and online spaces grows, the way we manage our information must also change. With a bit of diligence and care, you can safeguard your accounts and information. The good news: It doesn't take long, and a small investment of time will help you interact online with confidence.

Sejal Pattni
Global Head of Cyber
Education & Awareness
Cyber & Information Security

Common cyber attacks

As cyber criminals ramp up their activities, they're focusing their efforts on a small number of defined attacks. Being aware of these is the first step toward protecting yourself.

01 Phishing is when cyber criminals use e-mail to try to lure you into revealing your personal or confidential information by clicking a link or an attachment.

02 Viruses are malicious programs that attach themselves to authentic programs and run without permission on your computer or mobile/tablet device.

03 Social engineering is when criminals convince you to provide your personal or financial information under false pretenses, often by posing as someone they're not and preying on their victim's emotions.

04 Identity theft is the unauthorized acquisition and use of someone's personal information, usually for financial gain or to gain access to sensitive information.

05 Ransomware is a malicious program that blocks access to your computer, device or data, and demands that you pay a ransom to regain access.

Cyber perils

- 43% of cyber attacks are aimed at small businesses.[1]
- 40% of the small businesses that faced a severe cyber attack experienced at least eight hours of downtime.[2]
- 51% of social engineering attacks are phishing.[3]
- 3.1 billion spoofed e-mails are sent every day.[4]
- 37% of business were hit by a ransomware in 2021.[5]
- Data breaches rose to 68% last year to the highest total ever.[6]

[1] Source: The Cost of Cybercrime, Ninth Annual Cost of Cybercrime Study, Accenture, 2019.
[2] Source: Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats. Cisco, 2018.
[3] Source: Spear Phishing Report: Top Threats and Trends. Barracuda, 2022.
[4] Source: Gartner Report: What is Email Spoofing? Proofpoint, 2022.
[5] Source: Ransomware Statistics, Trends and Facts for 2022 and Beyond. Cloudwards, 2022.
[6] Source: 2021 Annual Data Breach Report Sets New Record for Number of Compromises. Identity Theft Resource Center, 2022.

How to create a policy to keep your family and family office cyber safe

When setting out to safeguard against cyber crime, creating a policy helps to spot vulnerabilities. You can draw up a document mapping your approach to staying secure.

In developing a cyber security policy, it's important to ask the following questions:

- What is the core data that you wish to protect? Just your data, or your family's, or the extended family's?
- How do you and your family access data? Is remote working a key part of your business model?
- Who else has regular access to the data to be protected? And do they have a legitimate "need to have"?
- What would be the impact on the family office if there was a confidentiality breach, compromising important data or making it unavailable?

Once you have answers to these questions, you can design your cyber security policy. The policy maps the rules, regulations and procedures you follow into a clear and concise document. It acts as a resource for employees, outlining how your organization stores, protects and disseminates information, as well as explaining what you expect from employees. Key topics may include:

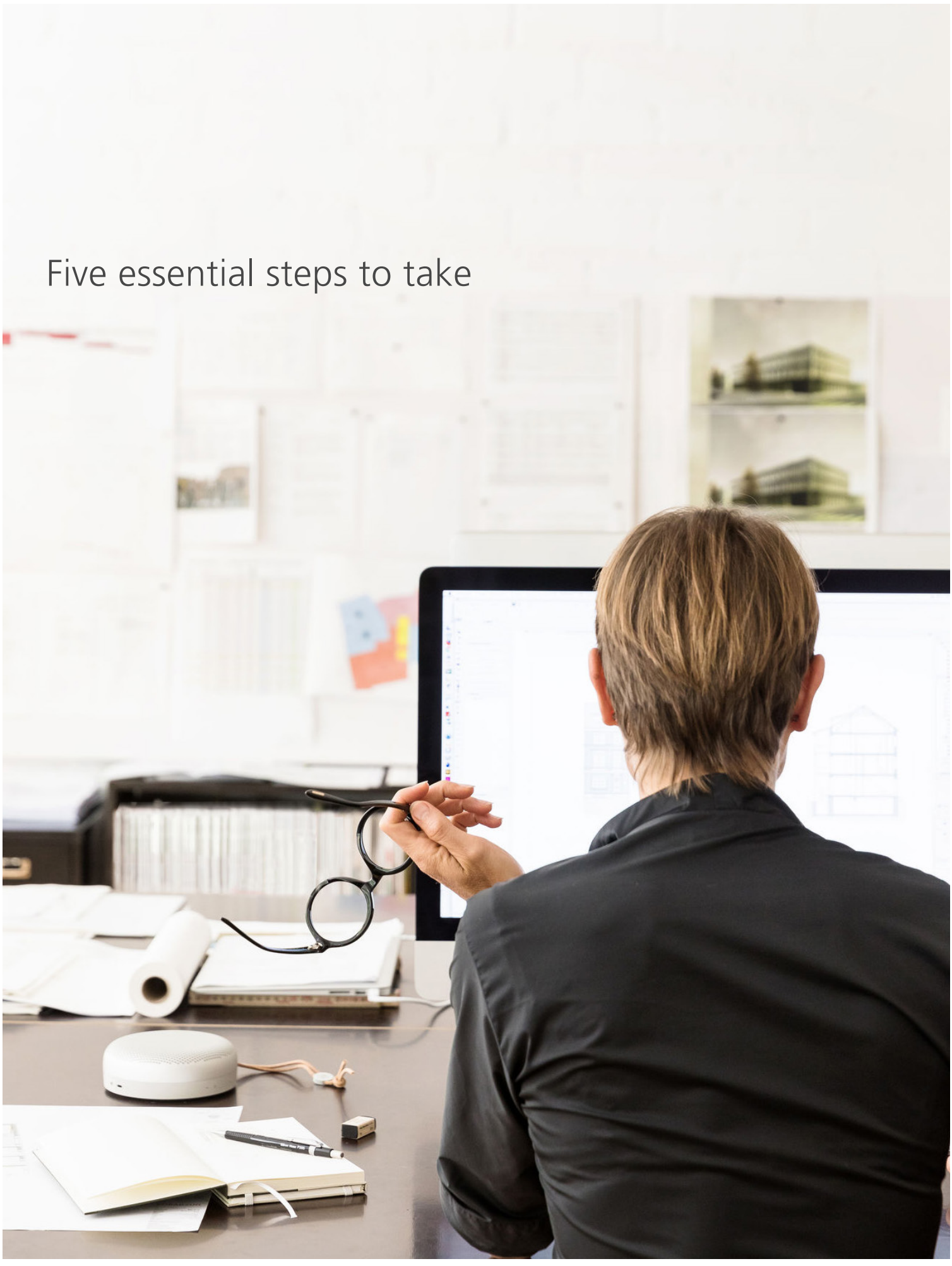
- How information is labelled and how it must be handled according to its sensitivity.
- How information is shared with third parties.
- Which security programs will be implemented (e.g., firewall, anti-malware, and anti-exploit software).
- How updates and patches will be applied in order to limit the attack surface (e.g., app updates).
- How data will be backed up (e.g., cloud, offline, etc.).
- How to handle a cyber security alert/breach of data, and how staff can report incidents.
- How to access the family office network and establish acceptable use.
- Social media guidelines.
- Managing legal and regulatory compliance.

Remember that cyber threats are constantly evolving, so it's important to review cyber security policy regularly.

Simple ground rules

- Avoid opening e-mails from unknown senders, downloading unexpected attachments or clicking on unfamiliar links.
- Use strong passwords and avoid sending personal or confidential information on unsecured networks.
- Secure your computer and devices by installing security patches and antivirus protection.

Five essential steps to take



1. Use multifactor authentication and unique passwords
Stories about data breaches are commonplace these days. From credit card systems to e-mail providers, it seems few organizations are immune to the world's most skilled hackers.

If your e-mail address and password are stolen from one organization, there's a good chance that the cyber criminals will try to use the same combination to see if they can access your bank, investment firm and other online services. In other words, account data lost in just one breach could make you vulnerable to identity theft, larceny and blackmail.

To avoid this fate, it's a best practice to use multifactor authentication where possible, combined with user names and passwords that are unique to every platform, including your social media, bank, e-mail and other online accounts. The strongest passwords are "pass phrases"—a long phrase that's easy to remember, but hard to guess. Aim for phrases longer than 14 characters for the best protection.

Using a secure password manager allows you to access dozens of websites and apps with a single password, despite having different usernames and passwords for each account.

2. Secure your home and small business networks
When setting up your home or business Internet, first change the default administrator password of the device controlling your wireless network. Second, enable encryption on your Wi-Fi router, preferably WPA2, (the second generation of the Wi-Fi protected access wireless security protocol). This security mechanism ensures online activity in your network is encrypted. And, finally, only allow people you trust to connect to your wireless network. Creating a strong password prevents others from connecting.

Not sure how to do this? Ask your Internet service provider, check its website, read the documentation that came with your home equipment or refer to the vendor's website (most vendors post user manuals).

3. Harden your devices
Device hardening means reducing vulnerabilities in your security devices. Proper management makes it harder for hackers to attack your devices (laptops, cell phones, tablets). There are some straightforward measures you can take:

- Only install applications from trusted sources, such as app stores or known websites, and delete applications you no longer need or don't know the origin of.

- Keep your applications and operating systems up to date, applying the latest security patches. Install anti-malware software on your Windows and Mac computers.

- Don't plug suspicious USB devices, such as unknown flash drives, into your computer.

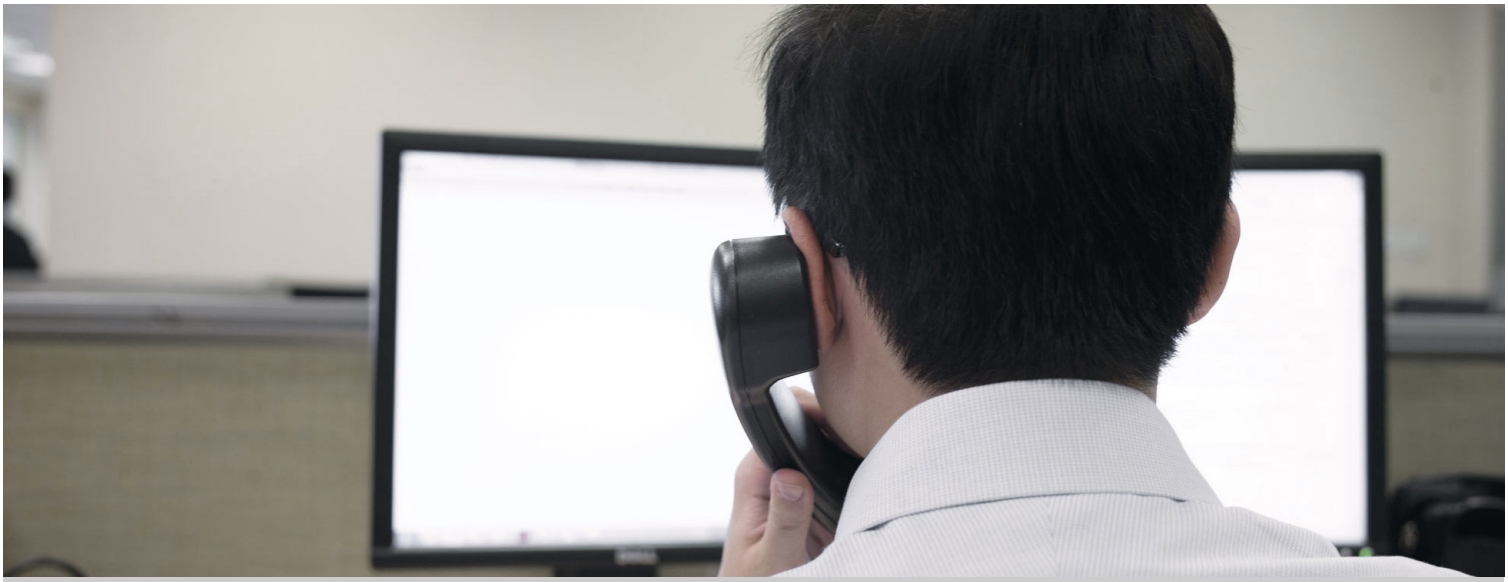
- Use your cell phone data instead of public Wi-Fi when on the go. If you must use public Wi-Fi, a virtual private network can ensure that your network traffic isn't intercepted or tampered with.

If your device has been stolen, Apple, Android and Windows' apps can all track its location and remotely wipe your data. Be sure to set up strong passcodes for unlocking your devices and use timers to lock them after a period of no use. That way, if someone does get hold of one of your devices, you can rest assured they won't gain access to your data.

4. Back up your important files
Ransomware is a type of malicious software that has been around for almost two decades and is designed to block access to a computer system or data until you pay a sum of money. Hackers are making easy money … so ransomware is growing fast. Even if you pay the ransom, there's no guarantee that you'll regain access to your device.

It's important to regularly back up important files, like family photos and financial records, to a secure cloud. Also back them up manually via an encrypted external hard drive. Strong back-up practices keep your files safe from both viruses and cyber criminals.

5. Be alert to social engineering
Deepfakes are becoming common, and hard to spot. A deepfake is a form of manipulated video and audio that creates hyperrealistic, artificial intelligence-generated voices and video of real-life people. It can be very misleading.
Be alert and apply the same diligence to scams like this as you would to phishing e-mails. Think twice before clicking any unusual links online, and if you're suspicious about someone you've spoken to, pause and call them back—using a phone number you have on file—to validate any request.



Port out scams

Your phone number is valuable information to a hacker, especially for a cyber attack known as a "port out" scam. In these instances, the hacker is looking to gain access to your bank accounts by taking over your phone number. However, they may also use it to try access your other online accounts as part of an identity takeover. While hackers are clever, it's possible to stay a step ahead. Here's what you need to know:

How it works

As a first step, the hacker will obtain personal information about you: e.g., address, family relations, bank details, etc. by using social networks, online databases, mining stolen data or even the old-fashioned way of collecting discarded physical documents. Using this information, they impersonate you and convince your phone company to switch ("port") your number to an account they control. This means that text messages that would normally go to you go to the hackers instead. They then work quickly to take advantage of password reset services, where login codes are usually sent to your phone, in order to access your online accounts.

Spotting the signs

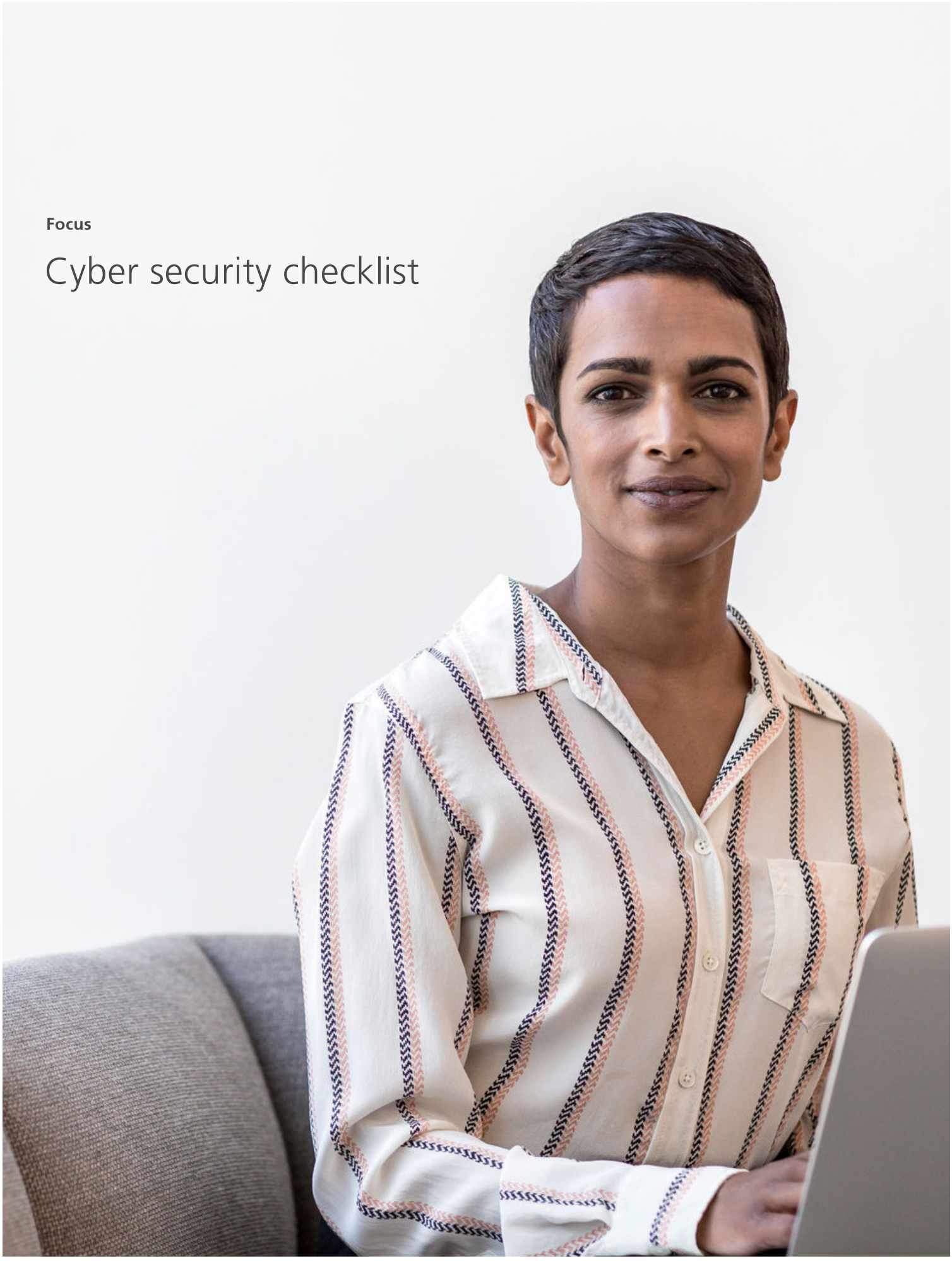
- You may get a text message or e-mail just prior to the "port" taking place.
- Your phone may stop working and/or your contacts may start to reach out to you in a different way, saying they're trying to reach you by phone.
- You're unable to access your bank and/or online accounts.

Keeping safe

1. Always question unsolicited e-mails, texts and calls. Clicking on links from unexpected e-mails and texts may allow hackers to access personal data, which they can then use to convince the bank and online institutions that they are you.
2. Don't overshare personal details on social networks, and regularly review your online footprint. Avoid posting your birth date, children's or relatives' names, memorable vacations, the name of your first pet or school, etc. These questions are common in password reset questions.
3. Securely shred sensitive physical documents.
4. Set up a secondary password or security code with your phone provider (if this service is offered). This will ensure that only you can port out your phone number. Make sure it's a unique, strong code or password that can't be guessed by checking out your online profile.
5. Inform both your bank and mobile phone provider if you unexpectedly receive notification of a PAC request (the process to transfer your mobile number) and/or your phone stops working normally.

Focus

Cyber security checklist



Cyber threats are here to stay. Use this checklist to help you and those you care about stay safe.

Browse the web and check e-mail securely

- Avoid using public computers or Wi-Fi hotspots when sending personal or confidential information.
- Only shop with reputable online vendors, and use credit cards or PayPal (not debit cards).
- Be careful about what personal information you make publicly available and send it only on secure websites ("https").
- Learn to recognize phishing; never open unfamiliar attachments or click on unfamiliar links.
- Ignore e-mails or text messages that ask you to confirm or provide personal information by replying to the e-mail or message.
- Use the filtering settings on your Internet browsers and search engines.

Manage your social media activities

- In your profiles and posts, avoid publishing personal information that is typically used for security or verification purposes, such as your full birth date or your mother's maiden name.
- Use privacy settings to control who can access your information, and review your privacy settings regularly.
- Accept friend requests only from people you know; only "follow" (not "friend") entities or public figures.
- Be wary of sharing your current location or future travel plans; never announce when you won't be home.
- Be careful about taking online polls or quizzes, or downloading apps that allow the organizer to access your account or data on your devices.

Strengthen your passwords

- Create passwords that are at least six to 15 characters long.
- Use a combination of special characters, numbers and upper and lower case letters.
- Avoid including personal identifiers, such as names or birthdates, in your passwords.
- Store your passwords securely and change them regularly, at least once every three to six months.
- Don't use the same password for all of your accounts.
- Consider the use of a password manager.
- Use multistep authentication procedures whenever possible.
- Do not allow "auto-save" of your passwords.

Protect your computer and devices

- Use a strong password and set your computer and devices to auto-lock after a short period of inactivity.
- Set all computers and devices for automatic software updates.
- Install up-to-date security software with antivirus, anti-malware and identity protections.
- Avoid keeping financial and confidential information on your devices unless necessary.
- Use file encryption for personal information that must be stored on your devices.
- Keep a copy of critical data on a separate, secure medium (e.g., an encrypted external hard drive).
- Do not allow text messages or caller ID to appear on your locked screen.
- Make sure you completely erase your hard drives prior to disposal.
- Make sure that an owner's permission and password is required to access your home Wi-Fi network.
- Create a security PIN to access your device.
- Turn off location services and unnecessary apps on your devices.
- Do not store or send personal or confidential information via e-mail or text.

Monitor financial statements and credit reports

- Request and review credit reports from each of the three national consumer reporting agencies regularly.
- Review your bank and credit card statements regularly, and look out for suspicious activity or unfamiliar charges.
- Review your Social Security Administration records annually.
- Go through your health claims carefully to ensure you've received the care for which your insurer paid.
- Remove your name from marketing lists, including for the three credit reporting bureaus (Experian, TransUnion, Equifax), to prevent unsolicited credit offers.
- Sign up for identify theft protection products or services, as appropriate for you.
- Place a fraud alert on your credit files if you are concerned that your personal or financial information has been compromised or misused.

Online reputation management

Increasingly, many day-to-day activities have a digital aspect to them, whether it be to oversee your finances, socialize or manage family activities. But did you know that every time you access online services you leave a digital footprint? Taken in isolation, each one of these "digital crumbs" may not be of value, but when combined, they could make for very interesting information—not only for marketers but also sadly for cyber criminals.

Digital footprints are created in two ways: Passively and actively

- A passive footprint is created when your data is collected, usually without you being aware. For example, search engines store your search history whenever you're logged in, and web servers log your computer's Internet Protocol (IP) address when you visit a website.

- An active digital footprint when you voluntarily share information online. Every time you send an e-mail, publish a blog, sign up for a newsletter or post something on social media, you're actively contributing to your digital footprint.

Managing your digital footprint is essential to safeguard your family office from cyber threats. Let's explore why:

01 Information might be used to guess your password, or to reset passwords using "forgotten password" options.

.

02 You might be impersonated. Fake accounts could be created in your name, using publicly available information and pictures.

03 You might even be socially engineered. For example, you could be the victim of a targeted phishing e-mail using a topic or theme that the cyber criminal knows interests you.

Three steps to managing your digital footprint

Step 1

Assess your online presence

Do your homework: Find out what information is available about you and your family online. Are you comfortable with the information available?

Step 2

Manage your digital footprint

Connections and social

- Remove metadata from photos before you post them online and always consider what's in the background. Metadata commonly stored in exchangeable image file format (EXIF) can reveal details about the location of the device the photo was taken with.
- Always think before posting online and take time before responding to something negative. Even posting about a vacation may tell burglars when your house is empty.
- Check privacy settings and customize them to suit your privacy levels.

Communications

- Always question an unsolicited contact and never click on links in e-mails if you are unsure about the sender's legitimacy.
- Be mindful of your communication channels. If you're using a new mobile or online chat channel, then its worth reading the terms and conditions to see how chat information will be stored and who has access.

Devices

- Think about app permissions. Check the storage locations and accessibility of data collected by the device. If possible, adjust settings so that your devices only share the information you want and when you want. Keep in mind that some apps collect information even when idle.
- Turn off any listening apps and devices (e.g., Alexa, Echo, etc.) that are near your office. Even change the activation word to one that you wouldn't normally use at work or in your private life.
- If you're giving away or trading your device for an upgrade, consider factory reset, which will erase all data.

Online accounts and browsing

- Enter as little authentic information as you can into online registration forms. And unless there is a legal reason to do so, do you need to enter details like your real name and birth date?
- Consider creating a separate e-mail account just for registering on online shopping sites. Keep this separate from any e-mail accounts linked to your financial accounts.
- Deactivate or shut any accounts that you no longer use.

Step 3

Continually review

Your information is a revenue source for numerous social media sites, advertisers and scammers. Privacy settings for such software, online accounts, apps and devices are often changed, exposing your personal information during upgrades or when new features are added. As such, it's a good idea to perform an audit to review what personal information (e.g., location, contacts etc.) applications have access to when they are installed or upgraded.

To keep an eye on your online presence, consider setting up an alert against your name (e.g., Google alerts). If you choose to use this service, set up a dedicated e-mail address as it will create a degree of separation from your other online accounts.

Useful resources:

- Google.com: A general search against specified criteria will include information hosted on a range of websites, e.g., LinkedIn.
- Google.com/images: Search specifically for images against search criteria.
- Google.com/groups: Search specifically for returns by a social media group against search criteria.

What to do when you find inaccurate or false information

If you find inaccurate information about yourself or your family online, then contact the owners of the website to have your information removed or corrected. It is recommended to:

- State clearly what you believe is inaccurate or incomplete
- Explain how the organization should correct it
- Provide evidence of the inaccuracies, if possible.

If the inaccurate information is on social media, then remove any tags linking you to the post. Contact the post owner to get the information corrected. In case of no response, you can contact the app administrators, or use "report issue" functionalities.

Protecting children and elders

In our digitally connected world, cyber criminals make no distinction between private and professional worlds and neither should you. Online security is as important at home as it is in the office: Families and caring adults should think about safety and security both online and offline.

Teaching children

Every child is taught basic safety and security, like not talking to strangers and looking both ways before crossing the street. Teaching young people easy-to-learn life lessons for online safety and privacy begins with parents and other adults leading the way.

1. Share with care—what you post can last a lifetime
Help children understand that any information they share online can easily be copied and is almost impossible to take back.

Teach them to consider who might see a post and how it might be perceived in the future.

2. Treat personal information like money. Value it. Protect it.
Information about children, such as the games they like to play and what they search for online, has value just like money. Talk to them about the value of their information and how to be selective with the information they share.

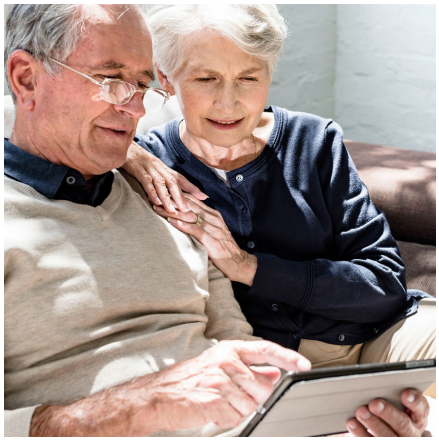
3. Post only about others as you would like them to post about you
Remind children and family members about the golden rule and that it applies online as well. What they do online can positively or negatively impact other people.

4. Own your online presence
Start the conversation about the public nature of the Internet early. Learn about and teach children how to use privacy and security settings on their favorite online games, apps and platforms.

5. Remain positively engaged
Pay attention to and know the online environments children use. In the real world, there are good and bad neighborhoods, and the online world is no different. Help them identify safe and trusted websites and apps.

Encourage them to be cautious about clicking on, downloading, posting and uploading content.

6. Stay current. Keep pace with new ways to stay safe online.
Keep up with new technology and ways to manage privacy. Visit trusted websites for the latest information about ways to stay safe online. Talk about what you discovered with children, and engage them on a regular basis to share what they know about privacy.



Helping elders avoid financial fraud

With cyber criminals, everyone is a potential target. Sadly, they target not only the young, but also the older generations and grandparents.

Why they are a target

The older generation didn't grow up with technology such as tablets and smartphones, which makes data so easily accessible these days. Further, they're more likely to have accumulated savings, investment portfolios and retirement accounts.

Types of scams they are subject to

The "grandma" scam is a technique that cyber criminals use to steal grandparents' funds. They find grandparents' phone numbers from publicly available sources, and then, with the help of social media, they might look for grandchildren. The hacker then calls the grandparent pretending to be a child, often citing some sort of emergency. A bad phone connection might heighten the drama. The hacker asks for money, preying on a grandparent's willingness to help a grandchild and the sense that it must be serious for the parents to be bypassed.

How to help your elders stay cyber safe

- Keep the dialogue open and talk to grandparents and elders about new digital scams. You can liken them to an old-fashioned "con man" but just in the online world.

- Set them up with good authentication. You could try a password manager, which will generate complex passwords for their accounts, and store them in a secure place so they don't have to remember all the different passwords. Even better—if you can set them up with biometric authentication, they'll be able to log into their accounts using just their fingerprints or facial recognition.

- Install security software and show them how to periodically update it.

- If something feels wrong, it probably is. Show them how to report anything that may seem suspicious. And if they receive a call pretending to be you or another family member/close friend, then tell them that it's OK to hang up and then to contact you via a known number instead.

Staying cyber safe in times of crisis

Cyber criminals sadly use times of crisis as an opportunity to get hold of your information through phishing attacks and other methods.

Here are some points to consider to stay cyber safe in such times, in addition to practicing good cyber hygiene:

Be alert to phishing e-mails and bogus calls
Some scams may reference a crisis situation or a global event, using emotion and urgency to entice you to reply or click a link. Check the authenticity of a request before sharing any information with people you don't know. Never click on any links, download any attachments or give information over the phone if you have any doubts.

Donate through official channels
Some scams may pretend to be fake charities, asking you to donate. If you wish to donate to a charity, it's best to make the donation by visiting the charity's official website, or by calling them on a known documented number.

Stay secure online
Only consult known, reputable sources for the latest crisis updates, and use multifactor authentication where possible. Don't click on advert links.

Conclusion

Enlisting a cyber security expert

In these times of escalating cyber crime, it's essential for every family and family office to take measures to prevent themselves from becoming victims. Should you choose to enlist a cyber security expert, he or she will be able to perform a vulnerability assessment, as well as advise you about what to do if you're attacked or your information is compromised online.

At UBS, we have experts who can provide advice. Similarly, our professional networks for clients can provide information.

Author biography

Sejal Pattni
Global Head of Cyber Education & Awareness

Sejal is based in the UK and is an Executive Director in UBS Cyber & Information Security.

Sejal has over 15 years of experience in financial services with various risk, governance and operational roles in the information and cyber security space. Her career has taken her on stints in Dubai, Western Europe and Africa where she has been involved in implementing security information policy, leading on risk assessments and implementing cyber training programs.

She manages the global cyber education and awareness program, keeping UBS staff appraised on key risks and how to stay cyber safe. She also leads on the development of frameworks to help build the next generation of cyber experts in the workforce.

Disclosures

This presentation is for informational and educational purposes only and should not be relied upon as investment advice or the basis for making any investment decisions or for any cyber and information security initiatives. UBS is not responsible for any compromise to the confidentiality, availability or integrity of client information. The views and opinions expressed may not be those of UBS Financial Services Inc. UBS Financial Services Inc. does not verify and does not guarantee the accuracy or completeness of the information presented.

Neither UBS Financial Services Inc. nor its employees (including its Financial Advisors) provide tax or legal advice. You should consult with your legal counsel and/or your accountant or tax professional regarding the legal or tax implications of a particular suggestion, strategy or investment, including any estate planning strategies, before you invest or implement.

As a firm providing wealth management services to clients, UBS Financial Services Inc. offers investment advisory services in its capacity as an SEC-registered investment adviser and brokerage services in its capacity as an SEC-registered broker-dealer. Investment advisory services and brokerage services are separate and distinct, differ in material ways and are governed by different laws and separate arrangements. It is important that you understand the ways in which we conduct business, and that you carefully read the agreements and disclosures that we provide to you about the products or services we offer. For more information, please review client relationship summary provided at ubs.com/relationshipsummary, or ask your UBS Financial Advisor for a copy.

 2022-761554
Exp.: 5/31/23; IS2202565.