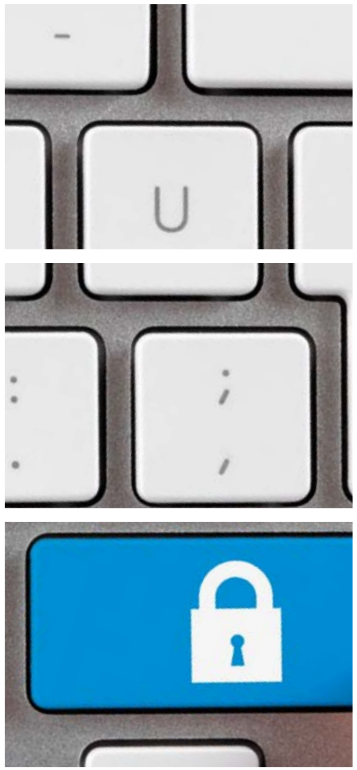
CREDIT SUISSE

Cybersecurity and You

Contents



Cybersecurity

At Credit Suisse, the security of your information is always a priority. We are committed to maintaining the security of our systems, software, networks and other technology assets against attempts by unauthorized parties to access or destroy confidential data, disrupt our services or cause other damage.

We have employees around the globe focusing on our cybersecurity efforts, including working with our regulators, law enforcement agencies and other businesses to maintain our defenses and enhance our resilience to threats.

Technology is rapidly evolving in a world driven by social networks, online transactions, cloud computing, and automated processes. But with technological evolution comes the progress of **cybercrime,** which continually develops new attack types, tools and techniques that allow these criminals to penetrate more complex or well-controlled environments, and produce increased damage and even remain untraceable.

For you, the Internet is quite possibly an integral part of everything you do; as a result, cybercrime is a growing and serious threat. Therefore it is **essential** that all of us consciously make fraud prevention part of our daily activities.

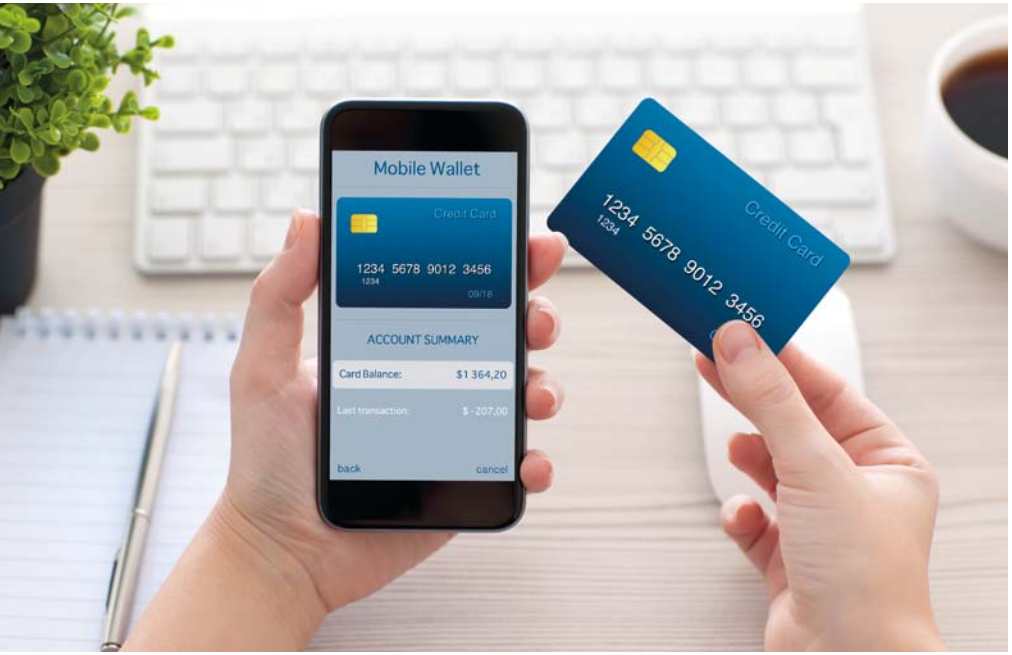
This booklet aims to remind you how to protect yourself, your assets and your personal information from online criminals.

Your cybersecurity checklist

A few reminders to keep your computers and money safe from online criminals

1. Have computer security programs running and regularly updated to look for the latest threats.
Install anti-virus software to protect against malware (malicious software) that can steal information such as account numbers and passwords, and use a firewall to prevent unauthorized access to your computer.

2. Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information.
Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they don't have up-to-date security software.



3. Get to know standard Internet safety features.
Install anti-virus software to protect against malware (malicious software) that can steal information such as account numbers and passwords, and use a firewall to prevent unauthorized access to your computer.

4. Ignore unsolicited emails asking you to open an attachment or click on a link if you're not sure who truly sent it and why.
Cybercriminals are good at creating fake emails that look legitimate, but can install malware. Your best bet is to either ignore unsolicited requests to open attachments or files or to independently verify that the supposed source actually sent the email to you by making contact using a published email address or telephone number.

5. Be suspicious if someone contacts you unexpectedly online and asks for your personal information.
A safe strategy is to ignore unsolicited requests for information, no matter how legitimate they appear, especially if they ask for information such as a Social Security number, bank account numbers and passwords.

6. Use the most secure process you can when logging into financial accounts.
Create "strong" passwords that are hard to guess, change them regularly, and try not to use the same passwords or PINs (personal identification numbers) for several accounts.

7. Be discreet when using social networking sites.
Criminals comb those sites looking for information such as someone's place of birth, mother's maiden name or a pet's name, in case those details can help them guess or reset passwords for online accounts.

8. Be careful when using smartphones and tablets.
Don't leave your mobile device unattended and use a device password or other method to control access if it's stolen or lost.

Personal cybersecurity at a glance

Protect your computer. Install software that protects against malware, or malicious software, which can access a computer system without your consent to steal passwords or account numbers. Also, use a firewall to prevent unauthorized access to your PC. While protection options vary, make sure the settings allow for automatic updates.

Use the strongest method available to log into financial accounts. Use the strongest authentication offered, especially for high-risk transactions. Use passwords that are difficult to guess and keep them secret. Create "strong" user IDs and passwords for your computers, mobile devices, and online accounts by using combinations of upper- and lower-case letters, numbers, and symbols that are hard to guess and then change them regularly. Although using the same password or PIN for several accounts can be tempting, doing so means a criminal who obtains one password or PIN can log in to other accounts.

Understand Internet safety features. You can have greater confidence that a website is authentic and that it encrypts (scrambles) your information during transmission if the web address starts with "https://." Also, ensure that you are logged out of financial accounts when you complete your transactions or walk away from the computer. To learn about additional safety steps, review your web browser's user instructions.

Be suspicious of unsolicited e-mails asking you to click on a link, download an attachment, or provide account information. It's easy for cyber criminals to copy the logo of a reputable company or organization into a phishing email. When responding to a simple request, you may be installing malware. Your safest strategy is to ignore unsolicited requests, no matter how legitimate or enticing they appear

Be careful where and how you connect to the Internet. Only access the Internet for banking or for other activities that involve personal information using your own laptop or mobile device through a known, trusted, and secure connection. A public computer, such as at a hotel business center or public library, and free Wi-Fi networks are not necessarily secure. It can be relatively easy for cyber criminals to intercept the Internet traffic in these locations.

Be careful when using social networking sites. Cyber criminals use social networking sites to gather details about individuals, such as their place or date of birth, a pet's name, their mother's maiden name, and other information that can help them figure out passwords—or how to reset them. Don't share your 'page' or access to your information with anyone you don't know and trust. Cyber criminals may pretend to be your 'friend' to convince you to send money or divulge personal information.

Take precautions with your tablet or smartphone. Consider opting for automatic updates for your device's operating system and "apps" (applications) when they become available to help reduce your vulnerability to software problems. Never leave your mobile device unattended and use a password or other security feature to restrict access in case your device is lost or stolen. Make sure you enable the "time-out" or "autolock" feature that secures your mobile device when it is left unused for a certain period of time. Research any app before downloading it.

Business cybersecurity at a glance

Protect computers and networks. Install security and antivirus software that protects against malware, or malicious software, which can access a computer system without the owner's consent for a variety of uses, including theft of information. Also, use a firewall to prevent unauthorized access. Protection options vary, so find one that is right for the size and complexity of your business. Update the software, as appropriate, to keep it current. For example, set antivirus software to run a scan after each update. If you use a wireless (Wi-Fi) network, make sure it is secure and encrypted. Protect access to the router by using strong passwords.

Require strong authentication. Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices, and online accounts by using combinations of upper- and lower-case letters, numbers, and symbols that are hard to guess and changed regularly. Consider implementing multi-factor authentication that requires additional information beyond a password to gain access. Check with vendors that handle sensitive data to see if they offer multi-factor authentication to access systems or accounts.

Control access to data and computers and create user accounts for each employee. Take measures to limit access or use of business computers to authorized individuals. Lock up laptops when not in use as they can be easily stolen or lost. Require each employee to have a separate user account and prohibit employees from sharing accounts. Only give employees access to the specific data systems they need to do their jobs, and don't let them install software without permission. Also, make sure that only employees who need administrative privileges, such as IT staff and key personnel, have them and regularly review their ongoing need for access.

Teach employees the basics. Establish security practices and policies for employees, such as appropriate Internet usage guidelines, and set expectations and consequences for policy violations. Establish a top-down corporate culture that stresses the importance of strong cybersecurity, especially when it comes to handling and protecting customer information and other vital data. Ensure that all employees know how to identify and report potential security incidents. Train employees to be careful where and how they connect to the Internet. Employees and third parties should only connect to your network using a trusted and secure connection. Public computers, such as at an Internet café, hotel business center or public library, may not be secure. Also, your employees shouldn't connect to your business's network if they are unsure about the wireless connection they are using, as is the case with many free Wi-Fi networks at public "hotspots." It can be relatively easy for cyber criminals to intercept the Internet traffic in these locations.

Train employees about the dangers of suspicious emails. Employees need to be suspicious of unsolicited e-mails asking them to click on a link, open an attachment, or provide account information. It's easy for cyber criminals to copy a reputable company's or organization's logo into a phishing e-mail. By complying with what appears to be a simple request,

your employees may be installing malware on your network. The safest strategy is to ignore unsolicited requests, no matter how legitimate they appear. Software vendors regularly provide patches or updates to their products to correct security flaws and improve functionality. A good practice is to download and install these software updates as soon as they are available. It may be most efficient to configure software to install such updates automatically.

Make backup copies of important systems and data. Regularly back up the data from computers used by your business. Remember to apply the same security measures, such as encryption, to your backup data that you would apply to the original. In addition to automated backups, regularly back up sensitive business data to a storage device at a secondary location that is secure.

Pay close attention to your bank accounts and watch for unauthorized withdrawals. Put in additional controls, such as confirmation calls before financial transfers are authorized with the financial institution. In recent years, there has been an increase in unauthorized electronic transfers made from bank accounts held by businesses. A common scam is an account takeover where cyber criminals use malicious software, such as keystroke loggers, to obtain the IDs and passwords for online bank accounts and then make withdrawals. Another scam called Business Email Compromise targets businesses by forging payment requests for legitimate vendors and directing the funds to the cyber criminal's account. Businesses are generally not covered by consumer protections against unauthorized electronic funds transfers.

Don't forget about tablets and smartphones. Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your business's network. If your employees connect their devices to the business's network, require them to password protect their devices, encrypt their data, and install security apps to prevent criminals from accessing the device while it is connected to public networks. Be sure to develop and enforce reporting procedures for lost or stolen equipment.

Watch out for fraudulent transactions and bills. Scams can range from payments with a worthless check or a fake credit or debit card to fraudulent returns of merchandise. Be sure you have insurance to protect against risks. Additionally, ensure that you report any irregularities immediately.

Email

Your email provider cannot guarantee your cybersecurity, and hackers attack providers to gain access to user accounts, or they directly attack individual email accounts using phishing, social engineering, malware or other scams.

Limit your exposure by maintaining separate email accounts for –

- Business
- Friends and family
- Important alerts
- For sites that require an email address as a User ID

In addition, to safeguard your information:

- Enable two-factor authentication in your email service when available to receive a text when there is a log-in from a new computer.
- Use data encryption to transmit personal information. Encoding the information makes it impossible for those without the encryption keys to read it.
- Employ spam filters to reduce the risk of malicious software and phishing scams (spam represents 65% of all email traffic).
- If you need to send someone a password-protected document, send the document in one email and the password in a separate email.

Social Engineering

Social engineering can leave you vulnerable to fraud Social media, such as Facebook or LinkedIn, can give hackers a wealth of information about you—which can be used to steal your assets or information.

- Limit the information you give out online. Criminals will search Facebook, Twitter and other social media for information about you and use it to defraud you, your family and/or your friends.
- Don't put personal/financial information in emails (or follow links sent to you in emails even if they come from trusted sources).
- Contact the email sender by phone or open a new email window (do not hit "reply") to ask the sender if the email you received is valid.
- Pay attention to the URL. Malicious websites look identical to real ones, but the URL may use a spelling variation or different domain (for example, does it say .net when it should say .com?)
- Don't enter sensitive information on websites unless you see proper security (the URL should begin with: https://).

Via telephone

Confirm an unknown caller's identity: Ask for the full and correct spelling of their name, a callback number, and an explanation for why the information is needed.

Be wary of impersonators: Validate the source through official public channels.

Do not supply information about other people: Have the caller contact the appropriate individual directly if you are asked for someone else's information.

In person

Be alert in public places for "shoulder surfers" who watch you entering personal information (such as PINs or passwords) in order to steal it and gain access to your accounts.

- Beware of people who try to enter a secure area with you without using their own authorization, such as a |badge or token.
- Do not insert unknown removable storage drives, such as USB sticks, that you have found or been given into your computer, as they may carry malware.

Internet

Hackers recreate well-known websites to capture your user credentials, such as passwords, Social Security numbers, credit card information, to name a few. They then use this stolen information to access your banking and other accounts.

Precautions to take online

- Make sure you keep your browser software up-to-date.
- Maintain a medium or higher level of security on your browser settings.
- Make sure the web address of any site you visit begins with https://. Some browsers show a padlock icon next to the https:// to indicate that you have a secure connection
- Remember: http:// is not secure.
- Log out after using an Internet banking or e-commerce service to ensure your session has closed
- Keep your cookies and browser cache clear so that hackers cannot access your history and obtain information.
- Remember that hackers increasingly target children on social media and gaming websites.
- Be mindful of the sites you visit: Do not visit sites that provide illegal downloads or illegal content (e.g., file sharing): Even if you do not download any files, you are vulnerable to viruses that can infect your computer.
- Keep pop-ups and ads blocked, and never respond to pop-ups asking you to submit or resubmit your log-in information.

Best Practice

- Regularly check your banking and credit card transaction histories and your statements for any suspicious transactions
- Use two-step authentication when it's available—you confirm your ID in two steps each time you use an ATM—with a debit card and PIN. Do the same online: Use a password and a code sent to you via text, email or call to access your account. You will receive an alert if someone logs in from a new computer.
- Avoid clicking either an ad's "close" button or anywhere within the window to close it.
- Enable private browsing whenever possible—prevent cookies and browsing history from being stored/saved to your device.
- Use trusted bookmarks for important sites—not email links or pop-ups
- Close windows containing pop-up ads or unexpected warnings using the X in the upper right-hand corner.
- Do not buy anything promoted in a spam message—even if it is a legitimate company, your purchase encourages spamming

Remember every device carries a risk. Laptops, tablets and mobile phones are all susceptible to wireless security breaches. Do not connect to sites you don't know or recognize. Don't assume a Wi-Fi link is legitimate; hackers create fraudulent

access points that appear to be identical to one that's legitimate. Instead, use a virtual private network (VPN), which allows only authorized users to access the network so data cannot be intercepted. Do not connect to sites you don't know or recognize.

Mobile Security

We have become more and more dependent on our smartphones and tablets for banking, shopping and social networking; therefore it is essential to protect your mobile devices. We should all be taking precautions to ensure these devices are protected.

Best practice guidance for your personal devices

- Adjust your security settings to restrict others' access to your data via wireless and Bluetooth connections.
- Avoid clicking on Internet ads: Ad-blocking apps exist for both Android and Apple devices, and browser settings can be adjusted to limit ad tracking.
- Update the apps on your device when new versions become available, as these often include security patches.
- If you think your device has been infected with malware: Contact either the device maker or your mobile phone carrier for help.
- Install a security app to scan and remove malware-infected apps.
- Do not try to bypass security controls in the device's operating system (i.e., don't jailbreak or root your phone).
- Keep your phone or computer locked - make sure it is password/PIN protected at all times.
- Keep the device's operating system software up-to-date and ensure you have the latest security patches.
- Encrypt sensitive information - if your mobile device or laptop has data encryption features, use them.
- Monitor how apps behave on your phone - keep track of permission access/requests from apps installed on your device.

- Use a reputable anti-malware/virus program and update regularly. Mobile devices are susceptible to the same risks as your home or office computers.
- Turn off Bluetooth when you don't need the connection - your device will be less vulnerable both to cyber-attacks and you will not drain the battery life.
- Choose a smartphone with anti-theft security features. If your phone is lost or stolen, having remote access to it will allow you to lock it, wipe the data stored on it and identify its location.
- Regularly back up your devices to your home computer or cloud network so that you have access to information if your device is lost, stolen or corrupted.
- Criminals use malware to steal or destroy your data—in the process, compromising the security and integrity of the equipment and/or systems you use. Don't ignore the warnings. Install antivirus software and pay attention to warnings you receive, such as when you are trying to access an unsafe site on the Internet.
- Be careful what you click and download. Clicking unfamiliar links can expose you to malicious software programs that scan your computer or track keystrokes, including passwords and account numbers.
- Some programs intentionally include malware. When installing, pay attention to message boxes and the fine print. Cancel any installation if you believe it may be harmful.
- Be wary of suspicious-looking email. Even email from people you know can contain malware links or attachments if their account has been compromised.
- Be careful following links in incoming email. Whenever possible, visit websites by entering the desired address directly in your browser.
- Scan files with security software before opening. Do not assume emailed files or those given to you on a disk or flash drive are safe.

Malware

Do not trust pop-up windows asking you to download software. Their goal is to convince you that your computer has been infected and that downloading the software will take care of the problem. Close this window immediately, making sure not to click on anything inside the pop-up window.

- Most file-sharing sites are illegal and should be avoided. There is very little policing for malware in these types of services. Malware can be disguised as a popular movie, album or program.
- If your computer is infected with a ransomware virus, in which a pop-up window appears informing you that your files have been encrypted in exchange for ransom, do not panic. Immediately disconnect your device from the network and try to restore your files from an earlier clean backup. Do not pay the ransom.

Notes

CREDIT SUISSE AG
P.O. Box 100
CH-8070 Zurich
credit-suisse.com

MCIZ 1 09.2017