Deutsche Bank

Security for your digital life

Editorial

Dear Reader,

Keeping in touch with friends, listening to music, searching for information, shopping and banking: we rely on the internet for so many things these days. Our smartphone and laptop are now always within reach, given that digitalisation has penetrated so many aspects of our personal and working lives. It has made many things much easier – and new things possible.

But at the same time, this networked world harbours risks which each of us has to address. New cyber-crime scams make headlines almost daily. These cyber-attacks are becoming increasingly difficult to spot and you could find yourself targeted – whether by phone call, e-mail, SMS or other message.

We have compiled this digital brochure to help make your daily digital dealings more secure. The nine chapters of this comprehensive digital guide contain all you need to know, with a wealth of concise tips.

You can find out how to protect your devices at home, your smartphone and access to your online accounts from page 4 onwards. Information on how to bolster your personal defences against phishing, fraud and psychological manipulation is provided as of page 20. Find out what really matters in terms of your security on social media and when shopping and banking online, and how you can help children and youngsters to keep themselves safe on the web.

Happy reading! Stay safe and keep well informed.

The Deutsche Bank Group

Table of contents

1.

Well protected online

Whether surfing, searching for information, reading e-mails, shopping online or exchanging news and views on social media, you should take care to ensure that your devices and accounts are protected from online attacks. Here are our tips for robust basic protection, secure passwords, routers, WiFi and cloud services.

Secure basis for your computers

Boost your computers' defences to enable them to better withstand cyber-attacks and ensure that your data doesn't provide cyber-criminals with easy pickings. Activate the lock screen function, even in familiar surroundings.

Updates

Always keep the operating system and all the software on your computers, laptops and tablets up to date. Not only do updates patch errors, but they also resolve security vulnerabilities that could otherwise be exploited by cyber-criminals.

1

It's best to activate the automatic software update function and ensure that the latest versions are not just downloaded, but also installed. The device often has to be connected to the mains to this end – and enough time allowed for the update to be concluded.

Only download software from trustworthy sources, and never by clicking on a link in a dubious e-mail or other message.

User profile

2 Create another user profile for daily use on computers and laptops, in addition to the user profile with administrator rights. If possible, the user profile with administrator rights should be used only to configure the device, otherwise there is a risk that cyber-criminals could seize control over the entire device in the wake of a malware attack.

Virus protection, firewalls and encryption

3 Install anti-virus software on your devices if no or insufficient protection is provided by the operating system. Always keep your software up to date and allow time for a regular, extensive and uninterrupted anti-virus scan.

Activate the firewall and hard drive encryption via the operating system to make it more difficult for your data to be misappropriated in a malware attack.

Browser

4 Update your web browser regularly as required and set it up securely. Activate the integrated phishing and malware protection. Make use of the data protection and security configuration options: for instance, you should not permit the browser to grant websites access to your payment options, contact data, camera and microphone without your explicit consent.

Backups

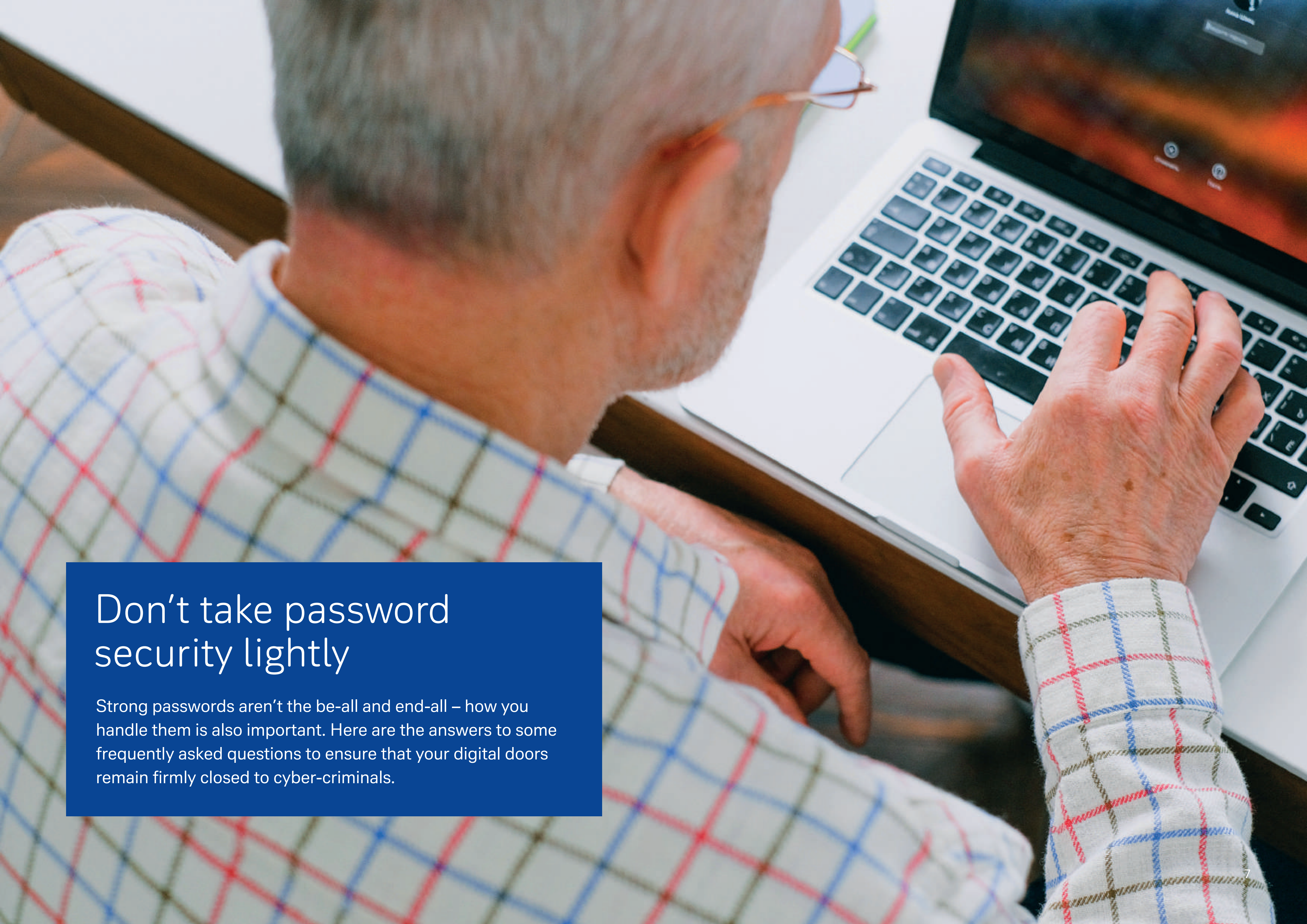
5

Create back-up copies of your data on external storage media on a regular basis. This will enable you to recover the data on your device if it is infected with ransomware following a cyber-attack or if the hard drive is broken. Hard drives are subject to wear and tear, so don't rely on a single hard drive as a back-up memory. You could also save additional copies to a cloud or on a second portable hard drive that is disconnected from your device once the back-up has been saved.

Device password and lock screen function

6

Lock your devices even in private surroundings if you happen to leave them unattended for a while, to prevent unauthorised persons from accessing your data and associated services. Make sure that the automatic lock screen function is activated. Use a secure device password and a biometric authentication method such as a fingerprint or the like.



Don’t take password security lightly

Strong passwords aren’t the be-all and end-all – how you handle them is also important. Here are the answers to some frequently asked questions to ensure that your digital doors remain firmly closed to cyber-criminals.

What makes a password strong?

Crooks try and get hold of passwords by technical means in brute force attacks. They use powerful computers and algorithms to try out passwords on log-in pages until they chance upon the right one. They can crack a six-digit password consisting only of lower-case letters in just six seconds using the processing power of a regular computer.

That’s why experts advise using considerably longer passwords. The length of a password depends on how many types of character it contains. The German Federal Office for Information Security (BSI) considers the following types of password secure:

- 20 to 25 characters made up of two types of character, such as a sequence of words comprising upper-case and lower-case letters that does not make sense. A password of this kind is usually easy to remember.
- 8 to 12 characters made up of four types of character: upper-case and lower-case letters, numbers and special characters.
- 8 characters made up of three types of character are sufficient if you use additional multi-factor authentication, which is generally recommended.

What is the advantage of multi-factor authentication?

Logging in with just your user name and password isn’t really secure. Anyone who knows the combination can log in to the account.

Multi-factor authentication involves a second process to establish that it is really you who is currently trying to log in: you are asked to provide something to which you alone have access. This may be a one-time code sent via an authentication app installed on your smartphone, or you might be required to confirm the log-in via a smartphone app or a biometric attribute such as a fingerprint.

Should I change my passwords regularly?

This advice is outdated, as it has been established that frequent password changes result in the use of passwords that are both too weak and too similar. The quality of the password is much more important. If the combination is secure, it should only be changed if you suspect that it might have fallen into the wrong hands.

I can’t memorise more than a handful of my passwords. What should I do with all the others?

A password is most secure if you can memorise it and never have to note it down or save it elsewhere. The best thing to do with all those that you can’t memorise is to save them in a password manager. This is much safer than noting them down or saving them in unencrypted form. They do not belong in the address book of your smartphone, in a Word document on a photo of a list of log-in credentials saved to your cloud.

Should I really use a different password for each of my accounts?

You certainly should. Let’s say that there has been a cyber-attack on the customer data of an online shop where you hold an account and that the crooks have managed to get hold of your log-in password. Hackers may attempt to use this same password to penetrate your e-mail account – and are likely to be successful if your password for both accounts is the same. This is because you presumably also have the same user name for both accounts, namely your e-mail address!

Why am I told not to share my passwords with others?

Because the risk of your password falling into the wrong hands and potentially being misused increases with every other person who knows it.

61 percent of all cyber-breaches are due to credentials having been compromised.

Source: 2021 Verizon Data Breach Investigations Report

How to prevent your router and WiFi from becoming gateways

Your home WiFi network and access to your router software are potential cyber-attack targets, as their passwords can be guessed by technical means. We explain what could happen and how to protect yourself.

If crooks manage to penetrate your WiFi network, they can read all of your data traffic and infect devices connected to your WiFi with malware. This gives them access to your data storage, computers and smart home devices such as cameras too.

Once hackers have taken control of your router, they can infect it and integrate it into a botnet with the aim of crippling websites. This will make your internet connection much slower. But worse could be to come: you might be taken to a fake log-in page when trying to log in to a website.

— So, you should certainly change the default password for logging in to the router software that has been set by the manufacturer and pick a password of at least 20 characters in length for both the WiFi and the router.

— The router software itself may by prone to vulnerabilities that can be resolved by updates. So, take care to update this firmware at least once a month if the device does not update automatically.

— Select a strong encryption standard such as WPA2 for the WiFi via the router software.

Off to the cloud – but take care

Cloud computing makes many things much easier and can even be more secure than saving data on your own devices. However, you should still weigh up the benefits and risks carefully. We explain what to watch out for in order to prevent unpleasant surprises.

With cloud computing, your software and files are no longer located on your computer's hard drive or in its working memory, but on the servers and systems of a cloud provider. You are using cloud computing when you set up a private e-mail account with an e-mail provider or listen to music via a streaming service.

Sending photos and videos wirelessly to the cloud from your smartphone and being able to retrieve them immediately from any other device? Saving every computer back-up automatically to the cloud in addition to the back-up copy on your portable hard drive? We'd all be reluctant to forgo these conveniences these days. But cloud computing enables us to do much more – and can be useful for a wealth of other personal aspects besides.

Saving documents, links and notes to a cloud where they can be retrieved by others from any location doesn't just make it much easier to plan holidays with friends. You might also wish to save medical diagnoses and other sensitive health-related data in order to enable doctors to access everything online in an emergency. You could even go one step further by using your browser to access special software that runs on an external system, for instance in order to complete your tax return.

In this instance, if not before, it should be clear to you that your data should not be entrusted to any old cloud provider – and that the more confidential the data in the cloud, the better protected the access to it should be.

Advantages and disadvantages of the personal usage of cloud services

+

- Data can be synchronised wirelessly across all devices, including address data, calendar entries, e-mails, photos and text files.
- Photos and documents can be made available to others easily.
- Shifting data to the server of a cloud provider frees up storage capacities on your own computer.
- Your data is still accessible if your own device breaks down, is stolen or destroyed – for instance during a burglary or house fire.
- Cloud applications for remote collaboration can also be useful for private projects, such as holiday planning or home improvements.
- You can also use special software without having to install it first – for instance for your tax returns or photo calendars.

−

- You don’t have any control over whether your cloud provider is protecting your data from cyber-attacks effectively.
- You may be unable to access data and software in the event of disruptions to cloud provider or internet provider services.
- The sharing of data saved to the cloud with other users may harbour security risks.
- Once you have set up cloud services on your smartphone, they are generally accessible without the need for any further log-in. But this means that anyone with access to your smartphone can also access data in your cloud.
- It can be difficult, or sometimes even impossible, to delete your own data from a cloud with immediate effect.
- The data privacy policy to which the cloud provider is subject can be less stringent in the case of locations outside the EU.

How to play it safe with cloud computing

- When choosing a cloud provider, look for security certification such as the “Trusted Cloud” label.
- Read the data privacy policy of a cloud service provider. Bear in mind that US intelligence services and security authorities have the right to access data of cloud users saved in US computer centres at any time.
- Only use cloud services that transmit your data in encrypted form.
- If possible, protect access to your cloud accounts via multi-factor authentication and keep your log-in credentials to yourself.
- Only release cloud data to others to a very limited extent. Bear in mind that links used to grant access to others could be intercepted by hackers if they are sent via e-mail.
- Save sensitive data such as copies of identity documents, bank and credit card information as well as health-related data only in clouds protected by high security standards and multi-factor authentication.

Tips for smart technology at home

Using an app to control your heating and lighting while on the go or checking cameras installed at home to ensure that everything is in order: smart home systems can make your life more convenient and secure, as well as help save energy costs. But these networked devices can become a security risk if they are vulnerable to attack by cyber-criminals.

What to watch out for when selecting and installing devices

— Prior to purchasing smart home devices, check whether the manufacturer offers security updates in the longer term. Well-known brands offer the best guarantees in this respect.

— Opt for devices that offer automatic software updates.

— If possible, connect your smart home devices to a separate WiFi network to which visitors do not have access and to which your computers and back-up memories are not connected either.

— Replace default passwords on smart home devices with individual passwords as a matter of priority.

— Only connect smart home devices to the internet if you really intend to access them from outside the home – otherwise you should disable the connection.

— If you can, protect the internet connection to your devices with a Virtual Private Network (VPN), to prevent hackers from tapping into the data traffic and ensure that only you can access the devices in question.

— In the case of voice-controlled devices, bear in mind that the device records everything you say and that all your utterances are processed and possibly saved by the system provider.

2.

All together under one roof

If you live in a household with several others, you share the WiFi and often computer and cloud services too. But this increases the risk of data falling into the wrong hands and providing cyber-criminals with easy pickings. Read on to find out how to prevent this.

Create a separate user profile for each person

If several people access a PC or laptop via the same user profile, it is hard to protect each individual's information and files effectively.

So, create a separate user profile for each person on shared computers. You can create additional user profiles via the operating system, specifying which data should be shared.

Configure separate WiFi networks

Friends and visitors should not be able to access computers, back-up memories and smart devices linked to your WiFi via your home network. Not only could they get hold of confidential data, but the devices linked to your WiFi could also be infected with malware via their smartphones.

So, configure a separate WiFi network for your friends and visitors. Call up the router software and create a WiFi network for your guests, selecting a strong encryption standard such as WPA2 and picking a separate password of at least 20 characters.

A separate cloud

Even if your family is happy to share most things, not all of your photos and documents are meant to be seen by your kids. So, use cloud accounts to which only you have access for your sensitive photos and documents, and keep the relevant log-in credentials to yourself. You can specify which content can be accessed by which other people via the release functions.

Set up your private cloud accounts to ensure that someone you trust can access them should something happen to you.

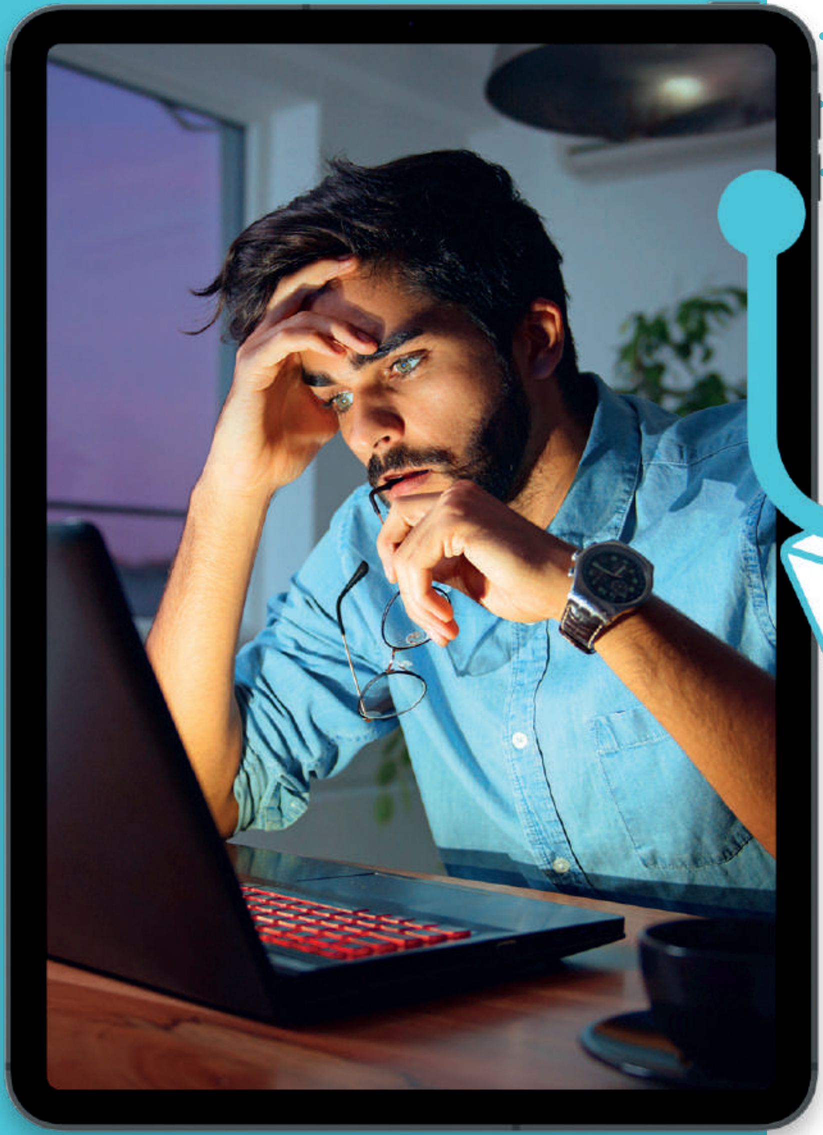
Sharing family passwords safely

Sharing passwords with others is, strictly speaking, taboo. But families and partners may find themselves having to do so – for the home WiFi network, for instance, or the family's music streaming subscription service. It might also be wise to give your log-in credentials for your private e-mail and social media accounts to someone you trust for use in an emergency.

What to watch out for

- Never send passwords and user names for an account in a single e-mail or even in two separate messages, as hackers might be able to access them.
- Always send the password and user name via two different channels, perhaps e-mailing the user name and sending the associated password by encrypted message.
- Ask the recipient to handle these log-in credentials securely.
- The use of a shared password manager via which specific access data can be released to other family members may prove useful within the family.

3.



Don’t be fooled!

Whether via e-mail, phone, messaging services or social media, cyber-criminals are always coming up with new tricks to extract log-in credentials from you or to con you into performing actions that will end up infecting your devices with malware. This type of scam is known as “phishing” – an amalgamation of the words “password” and “fishing”. Here we explain how to spot such attacks and protect yourself.

What does phishing aim to achieve?

The type of phishing with which most people are familiar is probably the fraudulent e-mail in which you are tricked into clicking on attachment or link under some spurious pretext.

If you do as instructed, you will often be taken to a fake website on which you are prompted to enter your password and other log-in credentials. But clicking on a malicious link can also result in you unwittingly downloading a malware-laden file that gives the perpetrators access to your data. E-mail attachments might also prove to be infected files.

Phishing attempts may also be made via text message, messaging service or social media with the same objectives in mind. Cyber-criminals might even phone you under a false identity with the aim of getting you to reveal sensitive information or otherwise do their bidding.

QR codes that you scan with your smartphone could also be malicious and take you to a fake log-in page or malware-laden download.

Are you alarmed or upset by the content of a message?

Then stop and think for a moment: don’t click on any attachments or links! Check whether the message is at all plausible and whether you can be sure of the sender’s identity.

Always be wary if a message seeks to play on your emotions. This trick is used by cyber-criminals to increase your stress levels and try to ensure that you comply with their instructions almost instinctively. They get in touch about allegedly urgent or alarming incidents and threaten you with consequences, or appeal to your helpful nature and make false promises.

Can you trust the sender of an e-mail?

Cyber-criminals frequently use e-mail addresses that are hard to distinguish from the genuine ones. Even if the e-mail has purportedly been sent by a well-known company, reputable organisation or person familiar to you, it could still be a fake.

So, always check whether the sender’s e-mail address is really correct. Pay close attention to every letter and every character! You should also be wary of private e-mail addresses created using a public e-mail provider account: cyber-criminals could have set up the account in the guise of another person!

Is the log-in page genuine?

Fake log-in pages on which you are prompted to enter passwords and other log-in credentials often look deceptively like the real thing. So, be wary if an apparently trustworthy e-mail takes you to a log-in page on which you are prompted to verify personal data in the wake of an alleged security problem or other incident. The e-mail in question will generally be a phishing e-mail.

This is not always the case, however, so always check the web address of the log-in page shown in your browser for possible fraud.

Fake web addresses aren’t always immediately recognisable as such: they often contain the familiar name or abbreviation of the company or organisation ostensibly responsible for the log-in page in question. However, this name or abbreviation is not positioned in the same place as it would be in the case of a genuine web address.

If you are to spot any deception, you need to identify the part of the web address known as the destination address, which might not be that of the ostensible sender. This is what to do:

Step 1

Starting at the double slash // in the web address, look for the next slash / on the right..
http(s)//some-random-words.destinationaddress.com/some-other-random-words

Step 2

Move backwards from this slash over the domain ending, e.g. “.com”, “.org” or “.de”, to the next dot to its left. Between this dot and the slash to the right of it is the destination address (highlighted in blue).

Step 3

Now check whether this destination address is correct. The best way of doing this is by using a search engine to call up the website of the company or organisation ostensibly responsible for the log-in page in a separate browser window. Find the destination address within the web address and compare it with that of the log-in page in question. If the two destination addresses are not identical, you have almost certainly exposed a fake log-in page.

A download link address can also reveal malicious intent, so perform the above steps on the link’s web address too. But don’t click on the link or download button – merely hover over it with the mouse to see the full web address.

Beware of spear phishing!

Not only can phishing e-mails be deceptively authentic as regards both layout and wording, but they might also address you by name and cite a pretext that appears highly relevant to you. This is known as spear phishing: the fraudulent message is addressed to you in person and might even refer to aspects of your personal or working life.

Spear phishing could be perpetrated by a social engineer who has gleaned a wealth of information about you and your life and is masquerading as a person you trust. You will find more information about social engineering as of page 26.

You should always be alert to the possibility that even an apparently highly plausible pretext in an e-mail could be anything but. Never click on any attachments or links if you have any doubts whatsoever!

Even an ostensibly legitimate phone call may be a spear phishing attack perpetrated by someone posing as a bank employee, software support staff member, police officer or security agent.

So, never reveal sensitive information to a stranger or disclose log-in credentials over the phone. Nor should you take the caller’s phone number on your display at face value – this number could have been faked and the caller may be phoning from a different number altogether.

Beware of dangerous file types in e-mails!

Cyber-criminals tend to favour certain file types when they want to infect your computer with malware: Word, Excel and PowerPoint files are particularly popular. All of them can contain what are known as macros – small programs in which malware can readily be hidden.

File packages with “.zip” extensions might also contain infected files, which you will be unaware of before opening the package in question. Programs featuring the extension “.exe” are also potentially dangerous, as they could harbour malware.

So, don’t open any Microsoft Office files or files with the extensions “.zip” or “.exe” if you have the slightest doubts about the authenticity of the e-mail via which they were sent. Your suspicions should be raised if you are prompted to enable macros or click on an additional button when opening an Office file. Don’t do it!

Malicious files and programs are not only found as attachments to e-mails and messaging service notifications, but can be smuggled onto your devices via download links in SMS and other messages too.

Keep abreast of the latest scams doing the rounds

Cyber-criminals are quick to exploit current events and situations and come up with topical new scams. So, pay attention to the latest phishing alerts issued by the police, security authorities, consumer organisations and your bank, and read the associated press reports. Here are some examples of common scams:

Fraudulent appeals for donations:

Crooks posing as aid organisations use social media to appeal for donations to support refugees fleeing the war in Ukraine.

Warning allegedly from Interpol or law enforcement agencies:

You receive a phone call from someone claiming that cyber-criminals are about to empty your bank account and instructing you to transfer the money to a trust account immediately.

Alleged IT glitch:

You are alerted to an alleged security problem by a someone claiming to work in IT support at Microsoft or another company and requesting remote access to your computer to resolve the issue. Beware: fraudsters are also quite capable of posing as IT support staff at your own company.

Fake invitations to video conferences:

Crooks exploit the fact that many people are currently working from home and reliant on remote work applications to send genuine-looking invitations to video conferences or notifications of voice messages that need to be retrieved. Details are promised when the recipients have entered their log-in credentials.

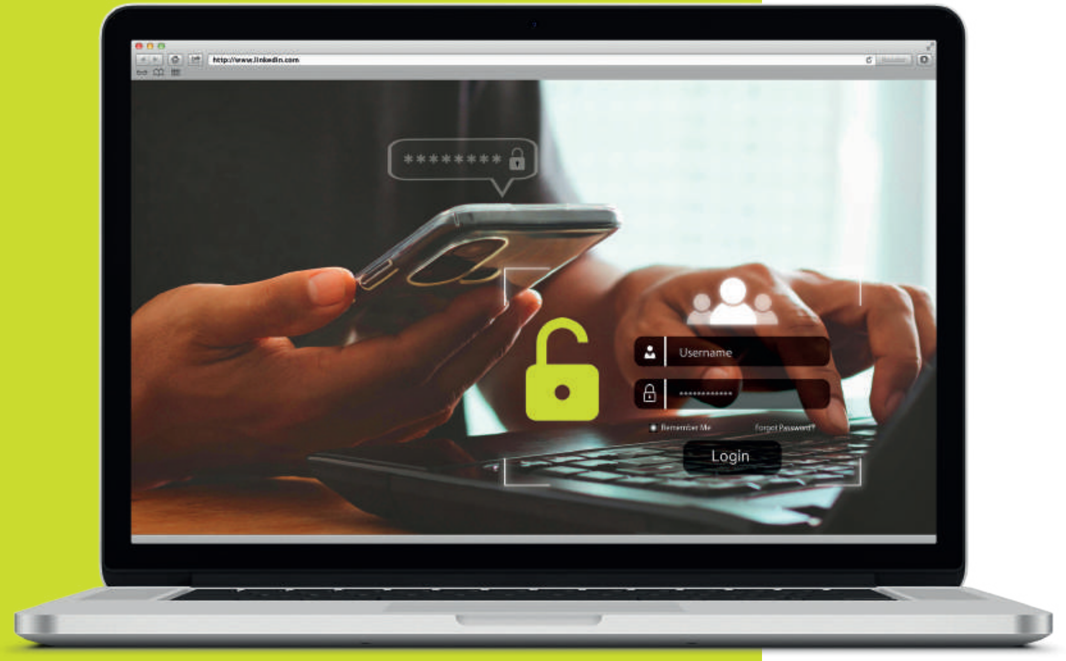
E-mail allegedly sent by your bank:

You are requested to verify account information on a fake website in the context of the economic sanctions imposed against Russia.

Text message allegedly sent by a parcel service:

You are asked to click on a link in the fraudulent message to see further details of a pending parcel delivery or to pay outstanding charges in this context.

4.



Planned well in advance

The ploys used by cyber-criminals are becoming ever more sophisticated. If an attack on a specific target is likely to pay handsome dividends, they are willing to spend plenty of time and effort spying on this individual and their life beforehand. On the basis of their research, they select a pretext that their target will find credible. We describe the machinations used by crooks to trick you into willingly doing things that you shouldn’t.

Hazards

You could encounter social engineering in various guises: as the carefully chosen target of a serious attack motivated by financial, economic, political or private gain, or as a victim tricked into divulging information subsequently used in an attack on someone else.

This all culminates in targets transferring a vast sum of money to a fraudulent bank account, clicking on a malicious link in an e-mail or text message, or revealing passwords or other highly sensitive information over the phone. Sometimes crooks are seeking to gain access to particular premises.

In cases where the stakes are high, the crooks prepare their attack intensively over a period of weeks, or sometimes even months. They start by searching for information on their potential target and their life with a view to creating a false identity and fake pretext for a promising ploy.

Of course, they benefit from the fact that a wealth of valuable information is freely available online. In particular, social media and professional networks such as LinkedIn are a treasure trove for crooks looking for information on a person's life, work, interests, relationships and plans.

The information gleaned here gives them ideas for the approaches to use in phone calls to people close to their target with a view to finding our further details. Beware: the perpetrators avail themselves of the all the tools of psychological manipulation when making contact in person.

Don't be taken in by attempts of this kind! Make it as difficult as possible for the crooks to gather information. Above all, always display a healthy dose of mistrust, because someone could be seeking to deceive or manipulate you at any time.

Possible profiles of a social engineer

- Police officer
- CEO
- IT support worker
- Catering employee
- New colleague
- Headhunter

Don’t let yourself be manipulated!

Social engineers avail themselves of fundamental principles of psychological manipulation in order to cultivate your willingness to keep in contact and get you to do their bidding. You should be wary if you notice any of the following patterns in any encounter with a stranger:

- Similarity:
  Social engineers attempt to establish a bond via things they ostensibly have in common with you – children of the same age, a pet, a shared name, hobby or belief.

- Authority:
  The crooks might pose as a member of a government agency or board member.

- Reciprocity:
  They ask a question, resulting in a personal conversation that you find congenial.

- Scarcity:
  They entice you with the prospect of an event or commodity that is ostensibly available only for a limited period.

- Consistency:
  The pretext used appears consistent and initially does not seem to require any further explanation.

- Consensus:
  It is made clear to you that it will be to your disadvantage if you fail to comply with the request.

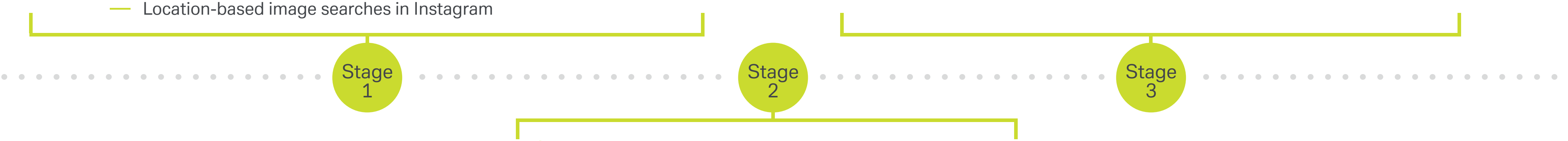
The five stages of social engineering

Social engineers typically proceed in distinct stages. The more information they can gather, the more effective their deceptive ploy is likely to be.

Procuring information from publicly accessible

Social engineers gradually work their way through the layers of information until they have an extremely detailed profile of their potential target. These are their typical sources:

- Websites and social media channels of companies, organisations and associations
- Profiles on business portals such as LinkedIn
- Private social media profiles, blogs and posts in forums
- Published photos of people’s homes and work, hobbies and holidays, friends, families and business partners
- Mapping sites such as Google Maps
- Location-based image searches in Instagram



Stage 1

Stage 2

Stage 3

Procuring information in person

Social engineers obtain additional details by contacting people close to their potential targets under a fictitious pretext.

- They get in touch by phone or e-mail.
- They may send a contact request from a fake social media profile so that they can view more than just the public posts and access contact data.
- They might also follow people in real life, for instance on public transport, and approach them in cafés or bars.

Devising a pretext

Social engineers then use the information acquired to devise a pretext that is likely to be accepted by the target immediately.

- They need to come up with both a suitable reason for getting in touch and a convincing role or identity to play in the attack proper.
- This role is fleshed out with various attributes and the purported résumé embellished with credible details.
- They might also decide to pose as someone you know, imitating the latter’s use of language in fake messages.

The five stages of social engineering

Stage 4

Establishing contact and the attack proper

Social engineers may initially make contact with the sole aim of establishing a strong relationship with their target:

- Via a fake profile on social platforms, dating sites or business portals.
- Via an e-mail designed to arouse the recipient’s interest in the purported sender.
- Via an e-mail containing information that is of interest to the target and announcing that the sender will be getting in touch.
- Via a phone call made with the intention of establishing a close bond with the target on the basis of personal or professional aspects that they ostensibly have in common.

If the social engineers are certain that they have a sound pretext, they may launch their attack proper without attempting to establish a relationship beforehand.

- They phone their target and engage them in a conversation, in the course of which the latter divulges sensitive information or expresses a willingness to do the social engineers’ bidding.
- They send their target a phishing e-mail from a fake e-mail address.
- They send their target an e-mail with instructions to transfer money to a bank account under their control.
- They use a pretext to gain access to particular premises.

Stage 5

Retreat!

Once social engineers have achieved their objective, they seek to cover up their digital tracks or to prevent their target from becoming suspicious after the event.

If they were previously in regular contact with their target, it is now time to withdraw on a pretext that appears plausible to the latter – either permanently, or until next time.

Don’t share everything

Prevent social engineers from gleaning information from your social media profiles that could be used to prepare an attack on yourself or others. Our section on social media as of page 33 explains how to protect your photos, posts and comments from being abused in this way as well as how to spot the fake profiles under which social engineers seek to establish contact.

Watch out for signs of spear

Are you addressed in person in an e-mail or other message from a stranger who is evidently privy to details of your professional or personal life? This could be a sign that social engineering is at play! Our section on phishing as of page 20 explains why spear phishing is so dangerous, how to check whether the sender’s e-mail address has been faked, and why you should refrain from clicking on attachments or links if you have any suspicions whatsoever.

Be suspicious of phone calls

- Never answer questions posed by a stranger unless you can be absolutely certain of the latter’s identity.
- Try to confirm the identity of the caller. Ask questions designed to establish the plausibility of the pretext for the call.
- Be wary if the caller refers to private matters, is evasive when questioned more closely or is not prepared to give you a phone number to call back.
- Avoid getting caught up in a lengthy conversation if you have any suspicions whatsoever. Ask the caller if you can phone them back. End the phone call and try and establish the caller’s identity and pretext for the call by means of other sources.
- If you have received a dubious phone call, discuss it with other people. You may not be the only person who has received one.

5.

Protect yourself and others!

Social media make it easy to get in touch with people, obtain information and exchange ideas and views. However, it's important to be aware of the risks involved in using these digital platforms. We explain how to protect yourself and others from unpleasant surprises.

Don’t make your private life public

Protect your personal privacy and that of others. Be aware of the fact that details from your private life could ultimately discredit yourself and others and be abused by social engineers, so think twice about what to post, share or comment on – and specify who can see that information.

Make sure that private information – such as details relating to marital status, family members, place of residence, travel destinations, hobbies and beliefs – are only accessible to people you really trust.

Limit the number of people with whom you share photos, posts and comments as far as possible. Visit your privacy settings and specify who can view what information. Create specific groups to this end if you can and specify a target group for each individual post. Only publish content of this nature after taking a conscious decision to do so.

Keep private affairs and business matters separate

Don’t publish any job-related information on private profiles without the blessing of your employer or customers.

There is otherwise a risk of confidential company information or details relating to your job ending up in the wrong hands. Even a photo of a business trip, your office or a meeting could pose a risk if a social engineer happens to be spying on you and your company. Refrain from identifying customers, employees or managers by name.

Hide your status information

Publicly visible information on your profiles could provide crooks with handy hints for future crimes.

Don’t let everybody see whether you are currently online, your current whereabouts, what you look like, or who your “friends” and “contacts” are. Your contact details, in particular, should not be made public.

In your profile settings, specify what status information is visible to whom and how your profiles can be located. To be on the safe side, you can conduct an internet search on another computer to find out what your profiles reveal about you.

The risk posed by fake profiles

In social networks, there is a high risk of criminals contacting you under fake identities and false pretences. Social engineers create fake profiles to this end, or acquire the log-in details for the profiles of people you know. You can find out more in the section on social engineering as of page 26.

So, never accept a contact request in social networks or on business platforms without having checked the respective user profile carefully.

By accepting a contact request, you are granting this person access to your entire profile, including photos, contact details and other personal information.

A social engineer could use this to pinpoint you as a suitable target for a cyber-attack and to contact you to this end. Someone bearing a grudge could also use this information to discredit you.

In general, you should therefore be extremely wary if you receive a contact request from a complete stranger. It’s best to use your privacy settings to specify who is permitted to send you a contact request.

How to expose a fake profile

Check the profile photo. It might in fact show a completely different person or prove to be a stock agency image. Copy the photo and use the drag and drop function to perform a reverse image search via Google or tineye.com. Compare the information from the hits with the details of the profile in question.

Also search for the name of the account holder and further public profile details of this person online, comparing images, details of where they live and other reference points with the information in the profile.

If an account holder neither posts any content nor shares others’ posts, this could indicate that the profile is fake and might simply vanish overnight.

Don’t be deceived either by a huge number of contacts or by well-known names. Most people accept contact requests from individuals who are not personal acquaintances. It’s more important to establish whether you and the purported account holder have any contacts in common and to contact the latter for further details, if so.

Watch out for privacy rights and copyrights

Once you have uploaded and posted a photo, video or comment, it may be shared beyond your control and you can often no longer delete or hide it. So, always consider the possible current and future ramifications beforehand.

You could, for instance, violate the privacy rights of an individual by sharing content in which the latter is pictured or mentioned without their consent.

Only use photos or videos from another person if you have obtained the copyright owner’s permission. The latter is generally the person who took the photo or footage in question. You should also pay attention to any music played or artwork shown: copyright applies to these too.

Protect your social media profiles

Create a unique, strong password for every profile and set up multi-factor authentication wherever possible. Also have a look at our section on password security as of page 7.

Cyber-criminals will otherwise find it easy to gain access to your profiles. They could spy on you and your “friends”, or spread fraudulent or false information under your name.

Don’t believe every social media post you read

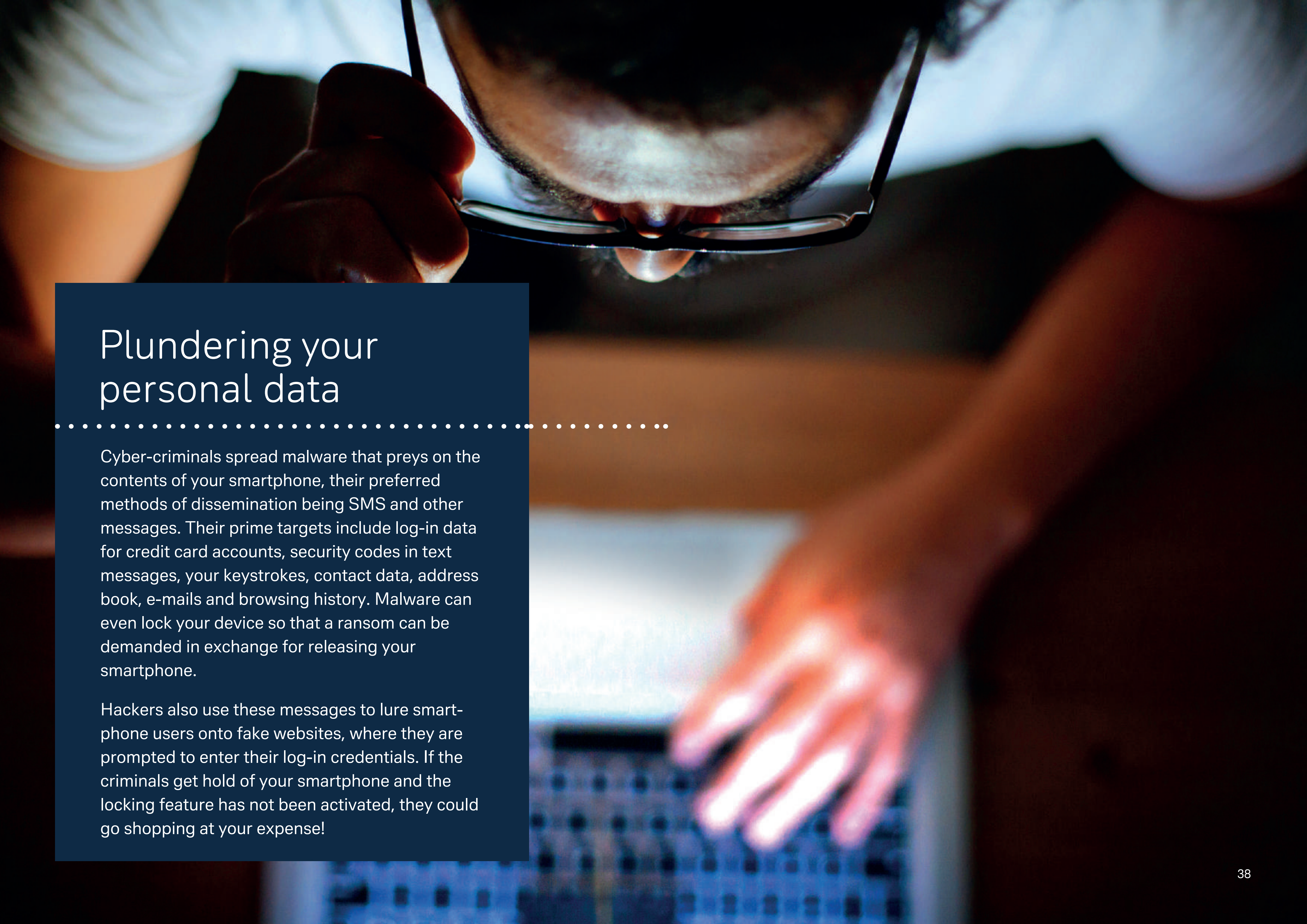
Don’t be manipulated by people who spread lies and conspiracy theories. Check the facts using other sources.

Be wary of links contained in posts, in or under videos, or in messages you receive – phishing could be at play here. If you click on these links, you could end up unwittingly downloading software or calling up a fraudulent website.

6.

Your whole life in your pocket

Can you imagine getting through the day without your smartphone? Probably not – staying in contact, obtaining information, sharing photos, buying and paying for things online – the smartphone is the central hub of our digit al world. And this is precisely why it has become a prime target for cyber- criminals. We explain how you can protect yourself against data theft and fraud, and how you can make online banking via smartphone even safer.



Plundering your personal data

Cyber-criminals spread malware that preys on the contents of your smartphone, their preferred methods of dissemination being SMS and other messages. Their prime targets include log-in data for credit card accounts, security codes in text messages, your keystrokes, contact data, address book, e-mails and browsing history. Malware can even lock your device so that a ransom can be demanded in exchange for releasing your smartphone.

Hackers also use these messages to lure smartphone users onto fake websites, where they are prompted to enter their log-in credentials. If the criminals get hold of your smartphone and the locking feature has not been activated, they could go shopping at your expense!

Always activate the lock screen function

If criminals get their hands on your unlocked smartphone, they could access your data and penetrate all your online accounts if your user name is also your e-mail address.

So, choose a security feature such as a PIN or fingerprint to open your smartphone and activate the automatic lock screen function. If possible, use a long or strong password instead of a four-digit PIN, and make fingerprints of several fingers.

Ensure that message notifications are not shown on your lock screen, so that strangers are unable to get hold of confidential information in this way.

Install software updates promptly

As well as enhancing functions, updates will also patch any known vulnerabilities that could be exploited by cyber-criminals. So, activate the automatic download and installation of available operating system updates. Keep all your apps up to date too.

Bear in mind that your smartphone must be connected to your WiFi and charging device long enough to allow system updates to complete – for instance, overnight.

Is an updated gaming app suddenly trying to gain access to your address book? Make sure you restrict the access rights to your apps again after updating them.

Download apps from secure sources only

Apps from dubious sources may contain dangerous malware that can even hack into multi-factor authentication and lure you onto fraudulent log-in pages. Apps like these often appear in the guise of games, video players, and anti-virus apps.

Manipulated apps are normally disseminated via social media and messaging services. So, don’t be tempted into clicking on a download link! Down-load apps only from approved sources such as Google Play, Apple’s App Store or the Microsoft Store.

Be careful with public WiFi

Whether at an hotel, restaurant, airport or elsewhere, even if you are asked to enter a password in order to use a public WiFi hotspot, this does not mean that the connection is necessarily secure.

Crooks could eavesdrop on the content of your e-mails, which are usually sent or received in unencrypted form.

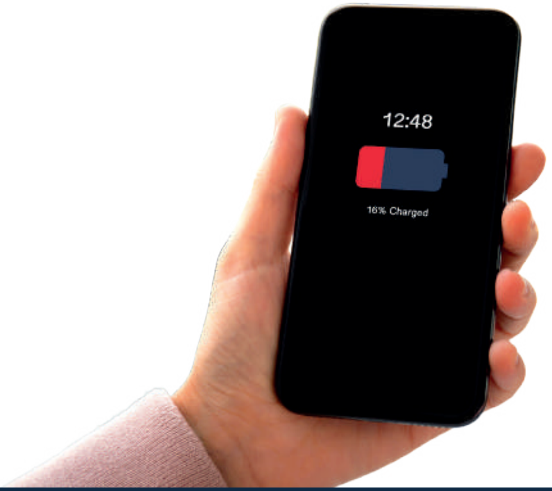
You should exercise particular caution in hotels and restaurants, where cyber-criminals may have blocked the guest WiFi and replaced it with their own featuring a fake log-in page. This fraudulent WiFi network could be used to infect your smartphone with malware. And when you call up a log-in page, you could be taken to a fake one without realising it.

So, refrain from sending e-mails, and steer clear of online banking and shopping if your smartphone is currently connected to public WiFi and you aren’t using a VPN. It’s safer to go online via your mobile data.

Don’t blunder into the subscription trap

Time and again, fraudsters will disseminate ads for games, adult entertainment, flirt groups and ring tones – hiding the fact that a subscription service will be activated the moment you respond by text message or phone call. You won’t see the true cost until you read your mobile phone bill!

You can take steps to guard against this: block third-party services with your mobile phone provider to avoid being billed for expensive subscriptions. You can normally activate third-party blocking via your mobile phone provider’s website. However, this won’t offer any protection against expensive in-app purchases!



Is your smartphone behaving strangely?

Be wary if your smartphone responds slowly, your data capacity is being used up quickly, and the battery life seems shorter than usual. Does your phone feel warm even though you’ve not been using it? Do unfamiliar apps keep opening?

These could all be signs that your smartphone has been infected with malware. It often places a huge strain on a phone’s processing power and internet performance as it is passing on information from the device without you noticing.

Don’t hesitate: reset the device and re-install the operating system and your apps. Change all your passwords!

Risk of SIM swapping ▸

One of the best known types of multi-factor authentication is the mobileTAN process, in which a text message containing a one-time code is sent to your smartphone. This type of authentication is particularly fraught with risk!

Cyber-criminals attempt to hijack people's mobile numbers with a view to intercepting the one-time code. This fraudulent takeover of mobile phone numbers is known as SIM swapping.

— You should take steps to prevent cyber-criminals from requesting and obtaining a new SIM card in your name. Protect your log-in to your mobile phone provider's website: pick a strong password that you use exclusively for this account and use multi-factor authentication if at all possible.

— Fraudsters might also attempt to identify themselves as you in a phone call to your mobile phone provider's call centre. So, keep your password for the phone service to yourself, and don't keep a record of it in the notes app of your smartphone or elsewhere.

— Disable the option that allows you to change the password for your mobile phone provider account or to unlock an account via text message. Contact your provider, who will help you configure your account settings.

— You should also configure your phone settings so that text messages are not displayed on the lock screen.

— Use a device PIN or device password to prevent unauthorised persons from accessing your smartphone.

There is no risk of SIM swapping if you use an authenticator app for multi-factor authentication, as this procedure is not linked to your mobile phone number.
Does all this sound far-fetched? Unfortunately, it happens far too often.
In 2021 alone, losses from SIM swapping attacks amounted to USD 68 million.*

** https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169*

Useful tips

When should I use a VPN?

If you often resort to public WiFi to reduce your monthly data usage, you should use a VPN (Virtual Private Network). The VPN will encrypt all data traffic, thus protecting it from cyber-attacks.

If the smartphone changes hands

Before handing a device over to its new owner, it is not enough merely to delete all the data and log-in passwords. The device is linked to the owner’s Google or Apple account in order to prevent a reset by thieves. If this link isn’t removed, the new owner will be unable to set the device up in their own name, while the previous owner will still be able to perform location tracking, lock the device and delete data.

Follow the detailed instructions for Android or iOS in preparation for handing a device over to a new owner.

If you are the new owner of a second-hand device, go to the system settings to check whether you can link the device to your own Google or Apple account. You will receive an error message if the previous owner has failed to remove the link to their own account.

Be careful with USB connections

Malware can get onto a smartphone not only via a manipulated charger or USB cable, but also via an infected computer that you have connected to your phone via USB.

7.

Online banking security

When it comes to online banking, the confidentiality of your data is accorded the highest priority. Deutsche Bank avails itself of the latest security standards to this end. Here we explain how you too can help ensure that this convenient method of banking remains secure at all times.

What should I always bear in mind when banking online?

1. Never log in to Deutsche Bank online banking from an unknown computer, especially not from internet cafés, where the computers are accessible to the general public.

2. Install anti-virus software on your computer: this will search for viruses and Trojans designed to spy on your log-in credentials. Always keep your anti-virus software, operating system and all application software up to date. Follow our instructions on basic protection for safe surfing as of page 4.

3. Enter the web address for your respective Deutsche Bank online banking access directly via the keyboard and make sure that you have just one browser window or tab open at the time. Then mark this address as a bookmark in your browser.

4. Refrain from using a search engine to find the address every time you want to sign in. There is a risk that you could click on a scam ad that takes you to a falsified log-in page. With these variants of phishing, criminals attempt to get a hold of your log-in credentials.

Can third parties read online banking data during transmission?

! No. In addition to the PIN/TAN process, all online banking transactions are protected by a special security protocol that encrypts the data. Deutsche Bank uses a globally recognised security standard known as SSL encryption to this end.

🔒 The padlock symbol in the browser bar indicates whether your online banking data is being transmitted in encrypted form. Click on the padlock symbol to check for the presence of certification issued to Deutsche Bank attesting to the authenticity of the communication partner.

How can viruses and Trojans threaten online banking security?

Malware may not be capable of attacking the security protocol for data transmission directly. However malware on your computer can lead to your log-in credentials being accessed by third parties. So, protect yourself against phishing (see page 20) and heed our security advice.

Why should I avoid a public WiFi connection for online banking?

Because there is a risk that this connection may be controlled by cyber-criminals and that you will be lured onto a fake log-in page or that your computer will be infected with malware. It is safer to go online via your mobile phone network when out and about. You can use the photoTAN app and Deutsche Bank Mobile app to transfer money via smartphone in just a few steps.

Why do Deutsche Bank customer PINs have just five characters and not eight or more?

A five-character PIN is safe for this purpose as long as it comprises both upper-case and lower-case letters and numbers between zero and nine. Hackers are unable to discover your PIN in a process of trial and error, as access to online banking is blocked following three unsuccessful attempts to log in.

To prevent your PIN from being guessed by people close to you, you should avoid the use of dates of birth, vehicle number plates and phone numbers, as well as the names of friends and relatives and words that are easy to guess.

Never save your PIN on your computer, smartphone or another device. We advise against the use of software that saves online banking log-in credentials on the hard drive in encrypted form.

Should I change my online banking PIN regularly?

Yes, at least once every quarter and also immediately if you suspect that your PIN could have been discovered by others.

Can I use the “auto-complete” and “save passwords” functions in my browser for online banking without jeopardising security?

No, that would be risky. You should disable any functions that allow the automatic entry and saving of information and passwords in a website form for reasons of security.

The mobileTAN process involves a TAN being sent to my smartphone via SMS for every transaction. What should I bear in mind?

If you use this process, you have to take particular care to prevent cyber-criminals from taking over your mobile phone number and intercepting the SMS containing the one-time code. This fraudulent takeover of mobile phone numbers is known as SIM swapping. See page xxx for details of how to prevent it.

Are there any current scams that I should be aware of?

E-mails sent to Deutsche Bank customers from fake sender addresses are currently doing the rounds with the aim of acquiring confidential customer data such as account numbers, PINs and TANs.

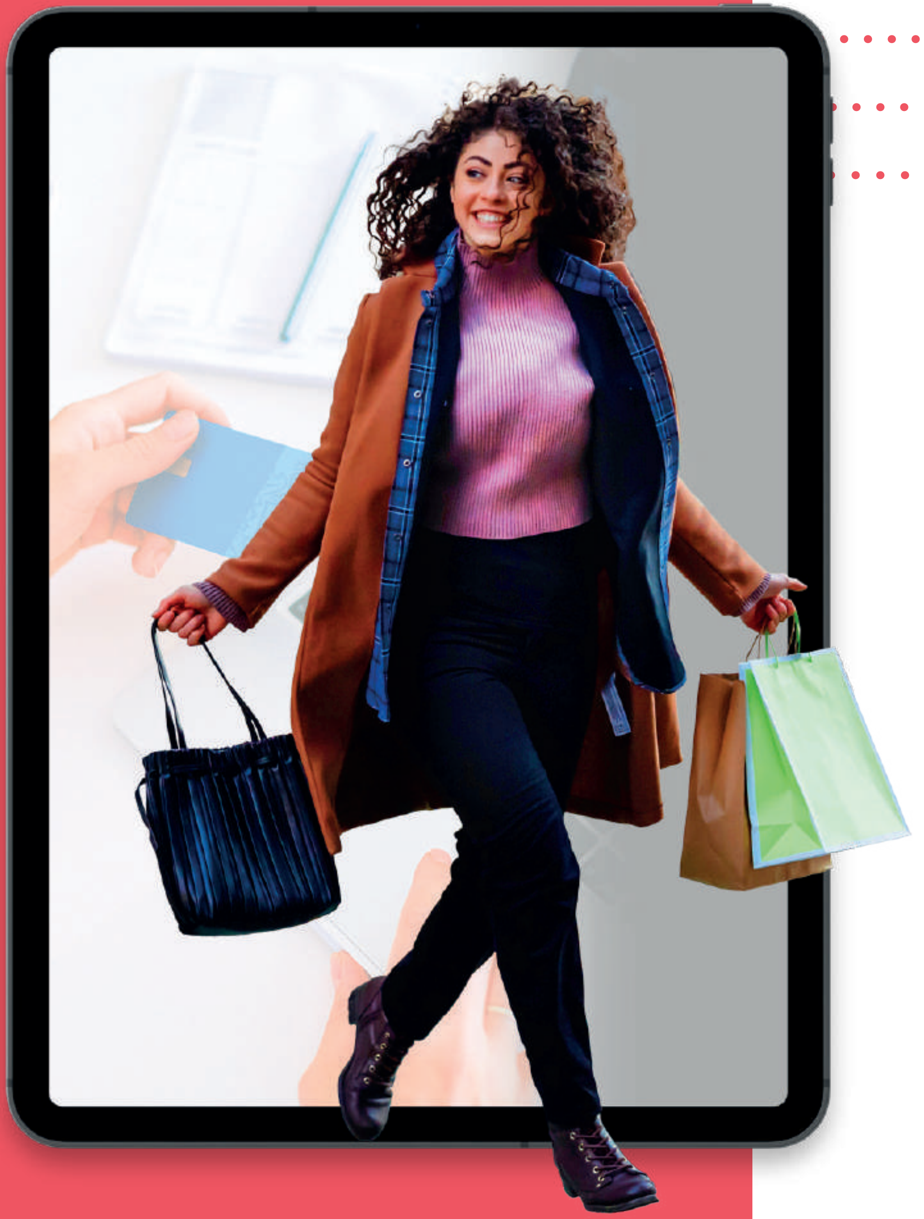
We still see phishing carried out primarily via e-mail and SMS messages (Smishing) for online banking, for example in the context of uploading a photoTAN activation letter. The following threats are also current and relevant:

- Fake calls of any kind (supposed Deutsche Bank employee, fake police officer, lawyer and so on) instructing the customer to authorise transactions.
- Grandparent scam via WhatsApp: Customers receive a WhatsApp message allegedly from a family member, often a child or grandparent, instructing them to settle a supposed account.

Please note: Deutsche Bank will never ask you for confidential data such as account numbers, PINs or TANs on the phone, by e-mail or text message, or request that you divulge such details by phone or e-mail or enter your log-in credentials. The Deutsche Bank online banking log-in page never requests one or more TANs.

Nor will Deutsche Bank ever send you an e-mail containing a direct link to the online banking log-in page! So, if you receive any e-mails of this kind, don’t follow their instructions.

8.



Online shopping without nasty surprises

Shopping online is both quick and convenient. But beware: a couple of clicks is all it takes to blunder into a trap set by fraudsters, and you might never see your money again. We explain how to spot fraudulent online shops and set out the advantages and disadvantages of various payment methods.

At first glance, you appear to have struck lucky: the price of the product you have your eye on is cheaper than anywhere else, or is actually available when it is sold out elsewhere. But your order is never delivered and your inquiries to the store operator fail to bear fruit: you are either fobbed off or simply ignored and will never see your money again.

Crooks can make millions with fake shops, which are becoming harder and harder to spot thanks to their increasingly polished used of language and professional layout.

The effort and expense required to create them is not excessive either. A fake shop can be taken offline as quickly as it appears online in the first place, with the fraudsters disappearing from view or pulling the strings from another continent. They are seldom apprehended.

Your money may not be the only thing that has been taken: the crooks could also have misappropriated your personal data and the payment information you provided so that they can go on a shopping spree at your expense.

So, take a close look at any online shop before making your first purchase – especially if the product price is exceptionally low, the product is un unavailable elsewhere or the features advertised appear too good to be true.

What contact information is stated?

Be wary if neither a contact phone number nor an e-mail address are stated on the shop website. A phone number which you will be charged for calling (often found abroad) or the presence of nothing more than a contact form could also indicate that this is a fake shop.

Are the company name, legal form and address stated? Don’t take everything you read at face value: use a search engine to check whether these details are plausible. The address might exist, but the stated company might not.

Are there any quality labels?

You will generally find well-known quality labels on the website of a reputable online shop. If you click on them, you will be taken to the respective portal to see information on the label in question. But the websites of fake shops will either not feature any quality labels, or the labels in question will be unclickable. Fake labels are also a sign of a fake shop.

Is the web address suspicious?

Look closely at the address of the shop as shown in the browser line. Only if it begins with „https://“ (the “s” standing for “secure”) and features a padlock symbol is the connection encrypted and consequently secure – this is standard in the case of trustworthy online shops. However, some fake shops also offer encrypted data transfer these days.

Fraudsters sometimes copy reputable online shops, using a web address that differs from the genuine address in just one or two details. You should definitely be on your guard if you spot suspicious endings such as “.de.com” or if the name in the web address does not match the shop offering.

The risk of being taken to a fake shop via a comparison portal is fairly low, although fraudsters often manage to ensure that their fake shops are easy to find via search engines.

What about the shipping costs and the terms and conditions?

Details relating to shipping, product returns and additional costs are often conspicuous by their absence on fake shop websites, as are the terms and conditions of business.

What do the customer reviews say?

Search online for reviews and ratings left by customers on rating portals and in forums. If the customer reviews and comments are uniformly positive, and are badly translated for good measure, this may well be a warning sign.

Which payment options are offered?

Most online shops offer a range of different payment options: purchase on account, by credit card or via a reputable online payment service. You should be wary if you are not offered any options apart from pre-payment when you try and complete your order.

Order now

Is the order button clear?

On the website of a reputable online shop, the button to confirm your order is clearly marked "Confirm order" or "Buy now". Ambiguous terms such as „Register", „Complete" or „Submit order" are not legally permitted and could be a sign that the shop is fake.

Which online payment method is the most secure?

Credit card

ⓘ The payment is authorised directly via the credit card number and 3D Secure process.

✓

- Payment method registered with the bank, no further user account necessary
- Multi-factor authentication makes it harder to commit fraud
- Fraudulent transactions can easily be reversed

✗

- Entry of sensitive information
- Risk of phishing attacks

Online money transfer

ⓘ The money is transferred immediately on confirmation of payment via the usual online banking data.

✓

- No separate registration with username and password required
- No entry of account data necessary

✗

- Payment service is positioned between customer and bank
- Sensitive account data is disclosed to the payment service

Pre-payment

ⓘ Payment of the invoice before the goods are shipped.

✓

- No online transfer of sensitive payment data to third parties

✗

- The transfer is very difficult to reverse in the event of fraud

⚠ Beware: you should only select this option if you have researched the online retailer in detail beforehand!

Which online payment method is the most secure?

Cash on delivery

Payment made directly to the parcel service delivery driver on delivery of the goods.

✓

- Goods are only paid for on delivery
- No online transfer of sensitive payment data to third parties
- Order is handed to the actual purchaser only

✗

- The payment is very difficult to reverse in the event of fraud
- Reimbursement options are complicated
- If the goods were ordered by fraudsters posing as your partner or family member and you have taken delivery of them in error, you will generally have no hope of reimbursement

Purchase on account

Once you have received the goods, you can decide whether or not to keep them – and only have to transfer the money afterwards.

✓

- No online transfer of sensitive payment data to third parties
- Goods can be inspected prior to payment
- Security level is high overall

✗

-

⚠ We advise using payment on account if possible.

Direct debit

Transfer of account data, with you authorising the debiting of the funds from your account via a SEPA direct debit mandate.

✓

- This direct debit authorisation can be cancelled within eight weeks of the funds being debited

✗

- Account data such as your IBAN and BIC have to be sent to the online shop
- Risk of phishing attacks

Which online payment method is the most secure?

Payment functions via operating systems

ⓘ

Payment via an app-based solution, with Google Pay and Apple Pay among the best-known services.

✓

- Payment data does not have to be entered for every online shop
- Payment data is not saved directly, but in the form of a token

✗

- All those authorised to use the device can also use the payment function
- Risk of phishing attacks

⚠ N.B.: you have to unlock your smartphone via a biometric feature or your smartphone PIN in order to make the payment. This means that the payment method is only as secure as your smartphone itself. You can find more information on smartphone security on page 37.

Internet payment provider

ⓘ

The payment is made via a payment service (such as PayDirect or PayPal) with which you have registered an account: the funds are subsequently debited from your bank account or credit card balance.

✓

- Payment data does not have to be entered for every online shop
- Payment data is not saved directly but in the form of a token

✗

- Multi-factor authentication is not a configured by default
- Risk of phishing attacks

⚠ N.B.: personal data and account details are saved with your payment service provider – so make sure that you take appropriate measures to protect them.

Protect your shop account

YOUR FAVOURITE SHOP

Sign in

Use your account to sign in here.

Email (phone for mobile accounts)

Password

Forgot your password?

Sign in using our secure server

By signing in, you agree to our privacy notice and conditions of use.

□ Keep me signed in. Details

New here?

Create your account

— Choose a separate, secure password for each of your online shop accounts. Use multi-factor authentication where possible and ensure that the internet connection is secure. You can find out more in the section on basic protection as of page 4.

— You must make sure that your e-mail account is well protected! Here's why: online shops generally require you to log in using your e-mail address as the user name. If crooks manage to access your e-mail account, they can use the "Forgotten your password?" function to request a new password for your online shop accounts, change the delivery address and go on a shopping spree at your expense.

— Don't save any payment data in your account if at all possible. You should delete the data for every shop account you no longer need via the customer profile or request its deletion.

9.

First steps for young internet users

Children require their parents' assistance in mastering safe internet use. We can help you to support your kids on their first forays into surfing and to keep them abreast of the risks they face as soon as they start to explore the web on their own.

Take your time and be the best coach that you can. Begin by going online together with your child and see where their interests lead you. They can gradually start to explore the internet on their own.

Keep confiding in one another so that you can point out the risks posed by such things as cyber-bullying and cyber-grooming, fake news and conspiracy theories, phishing, fake shops and hidden purchase traps. This will enable you to respond appropriately and support your child should anything untoward or even threatening occur.

Increase security via the special settings in your PC's operating system or additional apps to ensure that your child can surf the web in a protected environment.

Where to, my child?

The web is filled with pornography, violence, racism and hate speech: don't rely solely on technical filters to protect your child from inappropriate content. Together with your child, select the games and news sites it is allowed to access.

Consider making an online learning platform available for your child where it can access videos, interactive exercises and worksheets. Ask teachers or other parents to recommend good providers.

Make these websites the home page and favourites in your child's browser.

Select presets for children

Create a separate user profile for your child with age-based presets. This allows you to block inappropriate content and games, set screen times and avoid costly surprises.

On Windows computers, for instance, you can use Microsoft Family Safety to set up content filters and limit screen time. On Apple computers, you can create profiles for children and set screen time limits under System Preferences by clicking Users & Groups.

Setting boundaries on YouTube

Are your children often home alone? Then you shouldn't leave their video consumption up to them. YouTube offers a YouTube Kids app that makes it possible to specify which contents each individual child can access and how long the child is allowed to watch videos.

Create a profile for each of your children on youtubekids.com and make use of the protective settings. You can also specify that children may only watch videos and channels you have selected.

Raising awareness of phishing, identity theft and password security

Boost your child's capabilities in the field of "digital self-defence": make it clear what cyber-criminals' intentions are, what phishing attacks are designed to achieve, and which attack variants are worthy of particular attention – for instance, phishing e-mails associated with online games and gaming consoles. Describe the potential ramifications of having a profile hacked and spell out the basic rules of password security and the benefits of multi-factor authentication.

When children experience online abuse

There are many types of cyber-bullying: schoolchildren might post embarrassing photos or videos of classmates, or an entire group might make fun of somebody or ostracise them on social media. At worst, lies can be spread or the victim can be put under pressure, threatened or blackmailed. Encou-rage your child to talk to you about incidents of this kind.

Give your child the tools to tackle cyber-grooming by adults posing as children or young adults on fake social media accounts and making contact for the purpose of sexual exploitation. Promise your child that you will treat any revelations in this respect in confidence. The only proper course of action it can take is to swallow any embarrassment and discuss the issue openly with you.

Dodging the payment traps

Make your child aware of potential costs that could be incurred as a result of app or in-app purchases and subscriptions for online games and the like.

App and in-app purchases are generally paid for via the respective app store, so it's best to create a family account on Google Play or Apple's App Store. As its administrator, you can set up various types of purchase approval for other family members and approve or decline future purchase requests.

The costs for online game subscriptions, however, are charged to the mobile phone account. In many cases, it is not made clear that a transaction has taken place, especially where there is fraudulent intent. Some protection is offered by the third-party blocking option, which can be activated via your mobile phone provider and prevents subscription services from being charged to your mobile phone account.

When screen time becomes an issue

Don’t set rigid boundaries; instead, set time budgets that your child can use at its leisure. Make sure to set a good example in this regard: how much of your time at home do you spend in front of a screen?

When your child’s friends are already on social media

Sure, the grass is always greener on the other side! But that’s not how you should set the benchmark. The platforms’ terms and conditions require a minimum age of 13 or 16, depending on the country.

Legal information

While the content of this document ("Information") of Deutsche Bank AG or its group members ("DB") is believed to be reliable and has been obtained from sources believed to be reliable, the Information is furnished for specific information purposes only and is provided "AS IS" without warranty or representation of any kind. DB makes no representation or warranty that the Information (i) is accurate, current, complete or error free; (ii) satisfies any individual requirements of recipient including its fairness or reasonableness; or (iii) is fit for recipient's internal purpose. No legal advice, representation, warranty or condition, express or implied (whether by law or otherwise) is given by DB or by provision of the Information and all such representations, warranties and conditions are excluded to the extent that their exclusion is permitted by law.

DB may refer or provide links to third party websites or content in this Information ("Third Party Content"). The information, views and opinions expressed by such third parties and the authors of the Third Party Content are theirs alone and do not necessarily reflect the views, opinions or positions of DB and may not necessarily be consistent with DB's values, guidelines or policies. Should you identify any unsuitable or inappropriate Third Party Content, please contact DB for further assistance.

This Information contains proprietary information of DB or third parties. Especially, this Information and words, symbols, service marks or trademarks used in this Information are protected by trademark, copyright, database and other intellectual property rights owned by or licensed to DB and/or other third parties. Except with the express prior written permission of DB, this Information may not be published, disclosed, or used for any other purpose beyond the intended presentation. No part or parts hereof may be reproduced, distributed, adapted, modified, republished, displayed, broadcasted or transmitted in any manner or by any means beyond the intended presentation unless authorized by the owner.

This material is educational and thought leadership in nature and intended for the in-person Advisory Council hosted by Deutsche Bank Wealth Management. This is not material marketing any Deutsche Bank products or services and is not investment or financial advice.

“Deutsche Bank” means Deutsche Bank AG and its affiliated companies. Deutsche Bank Wealth Management refers to the wealth management activities for high-net-worth clients around the world conducted by Deutsche Bank AG or its subsidiaries. Brokerage services are offered through Deutsche Bank Securities Inc., a broker-dealer and registered investment adviser, which conducts investment banking and securities activities in the United States. Deutsche Bank Securities Inc. is a member of FINRA, NYSE and SIPC. Lending and banking services are offered through Deutsche Bank Trust Company Americas, member FDIC, and other members of the Deutsche Bank Group.