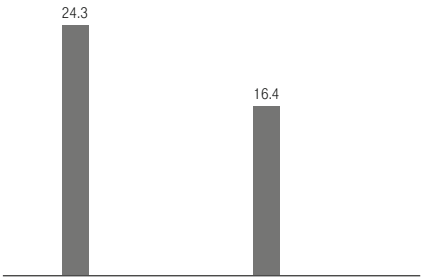
SURFING IN THE DIGITAL WORLD!
HOW TO PROTECT YOURSELF ON THE INTERNET

LIFE IS FOR SHARING.

SURFING IN THE DIGITAL WORLD!

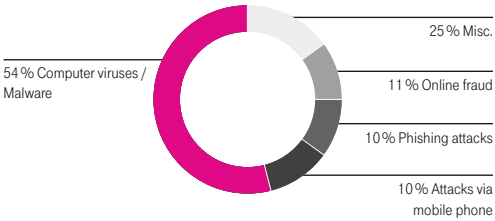
FINANCIAL DAMAGES RELATED TO CYBERCRIME

(BILLION €)



Data for Germany, Source: Norton Cyber-crime Report 2011

MOST COMMON TYPES OF INTERNET FRAUD



Data for Germany, Source: Norton Cyber-crime Report 2011

FOREWORD

It's hard to imagine life without the Internet anymore: We buy things online, chat with friends on other continents, stream films off the Internet – the possibilities are limitless. There's no foolproof way to guard against scammers, but we would like to show you how you can improve your safety with a few simple measures.

To make it easier to implement these steps into your daily life, we've developed a uniform symbol for data privacy. Wherever the magenta symbol appears, you know that an issue related to data privacy is involved. It points out data privacy tips or shows you which configuration options are available to make it safer to surf on the Internet.

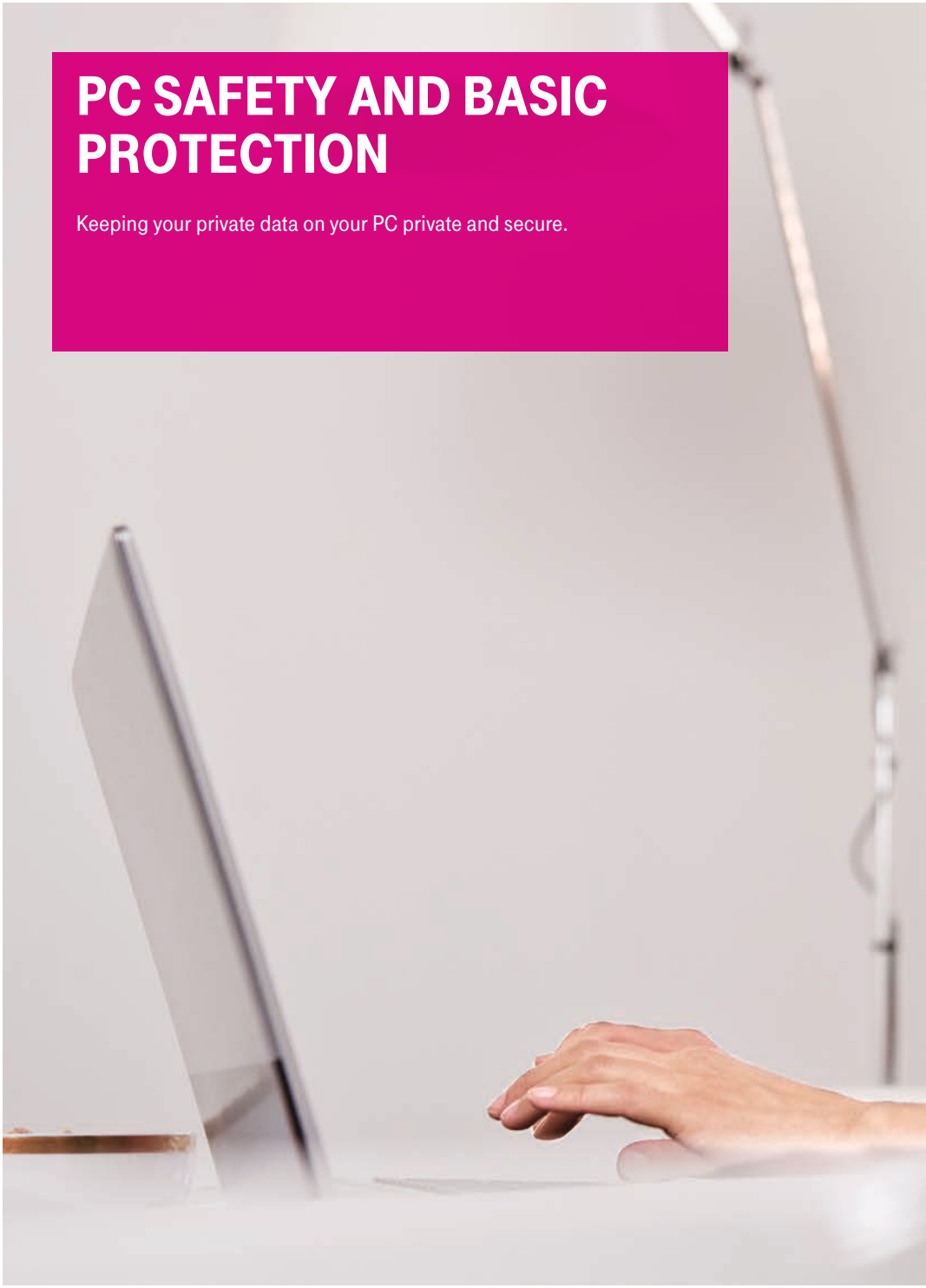
We've posted additional tips and tools are available at **http://www.telekom.com/dataprotection**. There you'll also find information about privacy protection and IT security issues as well as current threats on the Internet. If you have any further questions about data privacy or IT security, please feel free to contact us at any time on our website or via email (**privacy@telekom.de**).

Kind regards,
Claus-Dieter Ulmer

Group Data Privacy Officer
Deutsche Telekom Group

PC SAFETY AND BASIC PROTECTION

Keeping your private data on your PC private and secure.



ALWAYS BE AWARE OF HOW SENSITIVE DATA IS

Never input confidential information into a public PC, as you cannot be certain if it is properly protected against →**VIRUSES,** →**WORMS,** →**TROJANS** and other attacks. Protect your PC against prying eyes. Pay attention to who can see your screen before entering sensitive data such as user names or passwords.

ALWAYS KEEP YOUR SYSTEM UP TO DATE

Software providers are constantly upgrading their software to account for newly discovered security holes. Keep your software – and especially your anti-virus software – up to date to guard against attacks. Deutsche Telekom offers a security package to protect against attacks. The subscription runs on a monthly basis (**http://www.t-online.de/sicherheitspaket**, German only).

CONFIGURE YOUR SECURITY SOFTWARE RIGHT

Be sure to install both anti-virus and →**ANTI-SPYWARE** programs to protect your data. It's also important to set up a personal →**FIREWALL**. Proper settings protect you against attacks from the Internet. For Windows PCs, we recommend that at least activating the operating system's →**FIREWALL** and select the correct network type (home network or public network). Also use your email provider's →**VIRUS SCANNER** to achieve a greater level of security. Do not handle daily tasks on the PC using your administrator account; Create a standard account instead.

CHECK DOWNLOADS AND EMAIL ATTACHMENTS

→**VIRUSES** are commonly spread through file attachments on emails. Only open attachments from people you actually know. Similar rules apply to software downloads: if a provider or web page doesn't seem trustworthy, don't go through with the download.

SECURE YOUR PC WITH A PASSWORD

You should always use a password to protect your PC (and with it your data) against unauthorized third-party access. Make sure that the password is highly secure. The computer screen will unlock after entering the correct password and you can continue working. It's recommended that the screen and keyboard be set to lock automatically after five minutes of inactivity. For home computers, activation time is of course up to you. It's also possible to set the block to start immediately as needed. On a Windows operating system, this is initiated by pressing the key combination Ctrl + Alt + Del and selecting the option "Lock Workstation".

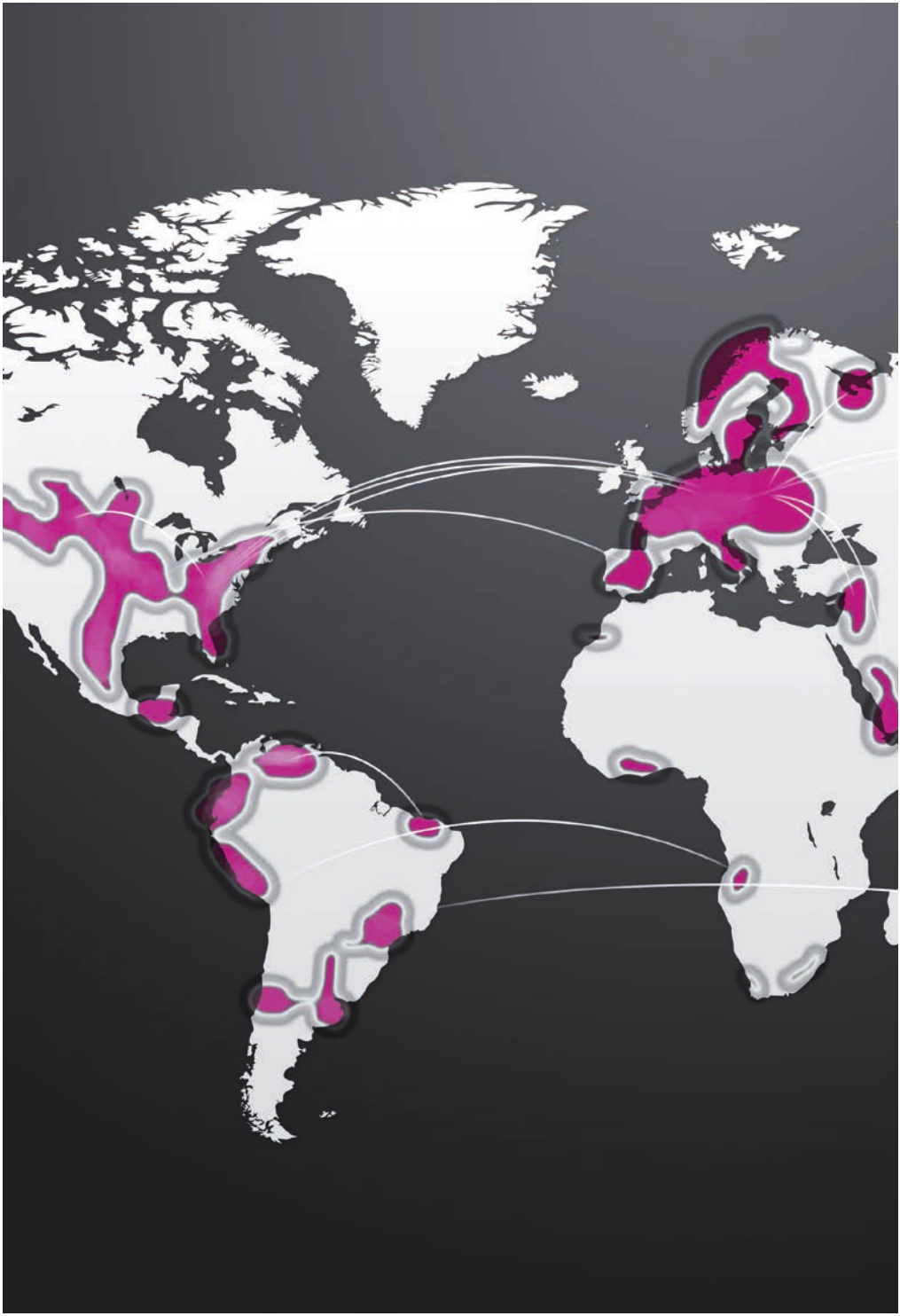
TURN OFF THE WIRELESS INTERFACES

To protect your private PC against external attacks, switch off all unneeded wireless interfaces – when you leave the room, turn off the lights as well! So, why not switch off the →**WLAN** transmitter from the router when you're not surfing the Internet? Most models today have a button on the back.

If other users need the same router, you can alternatively turn off the →**WLAN** receiver on your end device. It's easy to do, and saves energy as well. The same holds true for your cell phone – for example with your →**BLUETOOTH** port to protect it against →**VIRUSES,** →**WORMS** and →**TROJANS** and to prevent unauthorized users from gaining access to your personal data, including your address book, calendar and photos. Take care to always keep the →**WLAN** password on your router secret (see "Choosing a Safe Password").

DATA SECURITY

The safest approach is to create a backup copy of crucial data on a routine basis, such as on a CD-ROM/DVD or an external hard drive. Or use the Mediacenter available at no charge to Telekom customers and store your files on the secure TelekomCloud (see "Cloud Computing").



A PRIMER ON BOT NETS

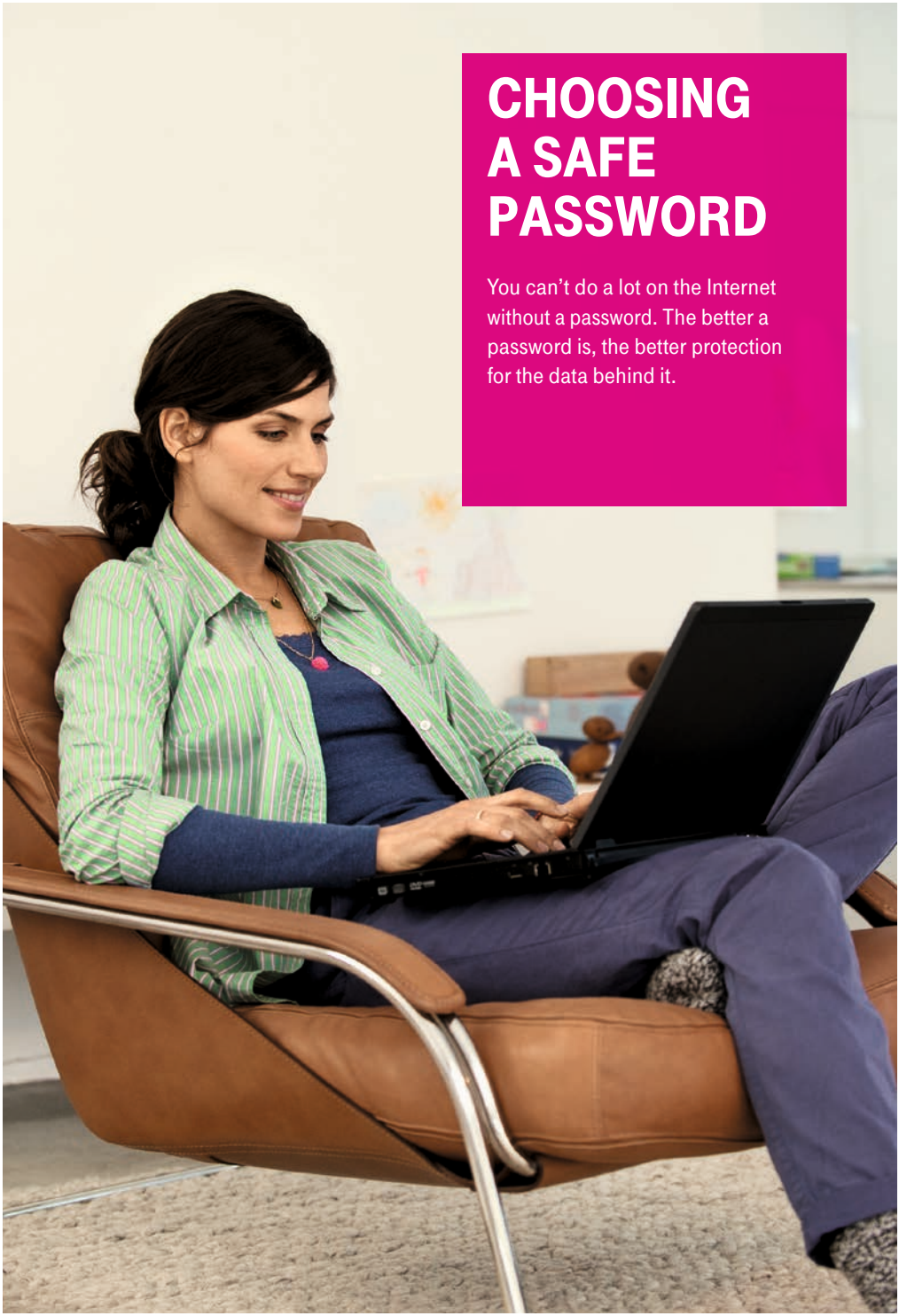
If your processor is a part of a →**BOT NET**, cyber criminals can control it remotely unnoticed and send out spam or infect other computers when you go online for example.

→**BOT NETS** are one of the cornerstones of cybercrime and are the biggest source of illegal income on the Internet. They are networks of computers that have been joined together after being infected with malicious software.

To protect yourself and others against this type of attack, follow the suggestions of the Anti-Botnet Advisory Centre (**https://www.botfrei.de/en/index.html**):

- Inspecting your computer for an infection. The DE Cleaner at **https://www.botfrei.de/en/index.html** detects potential viruses and deletes them.
- Keep the service packs on your computer up to date and activate automatic updates to receive the latest security updates for your system.
- Install a →**VIRUS SCANNER** and keep it updated regularly.
- Use a →**FIREWALL**.

https://www.botfrei.de/en/index.html is a website set up by the Anti-Botnet Advisory Centre of the German Federal Office for Security in IT. It explains what →**BOT NETS** are, the danger they represent and how to protect against them. The tabs “Information”, “Disinfecting” and “Prevention” provide all the information you need to protect your computer for the long run against malicious software.



CHOOSING A SAFE PASSWORD

You can't do a lot on the Internet without a password. The better a password is, the better protection for the data behind it.

Anyone who uses the Internet needs user names and passwords to access various forums and communities, as well as for online shopping. After the fifth password, it's difficult to keep track of them all. Beyond this, secure passwords are in many cases not memorable. But there is a solution.

HOW TO CREATE A SECURE PASSWORD?

The golden rule for a secure password: It should not be something that an outsider would even be able to recognize as meaningful! Here's one simple trick: simply select a sentence that's easy for you to remember, and then use the first letter of each word in that sentence to form a new word. To make the password as tough to crack as possible, supplement the sentence with numbers and special characters. For example: **"My mother buys 16 eggs every Saturday at the Farmer's Market" becomes "Mmb16eeSatFM!"**

The experts recommend that at bare minimum you use at least eight – as random as possible – characters, but it can be even longer. The golden rule: the longer and **more complex** the password, the better.

LOCKING OUT THE HACKERS

Here's why: Hackers use special programs that systematically try all the possibilities, how a password can be built. Each additional character added to the password raises the number of potential passwords – and with it the number of passwords that these computer programs have to run to try and crack your password.

CREATE DIFFERENT PASSWORDS FOR DIFFERENT APPLICATION AREAS

Another important preventive measure: where possible, use different passwords for different logins. As occasionally a data thief acquires complete customer data from including all access data.

A password that has fallen into the hands of thieves is no longer secure, as the thief will also use this password to try to fraudulently log into other accounts. A secure password is thus a password that is only used for one login. At any rate, this should be the case for your online banking password.

KEEP YOUR PASSWORD STORED SAFELY

You should only ever store your password in a secure location, where only you have access to. The most secure location, of course, is your head. The worst place is probably your browser. A better idea is to use password safe software like Passwortsafe, Keypass, lastpass, or 1Password. These programs can also generate secure passwords for you.

CHANGE IMPORTANT PASSWORDS REGULARLY

You should change important passwords at regular intervals to increase protection against data theft. We recommend that you change your passwords every three months or so.

WHEN DO YOU NEED A SECURE PASSWORD?

You may not always need a password that complies with the strictest safety standards. You probably don't have to be as careful with the fly fisherman's fan club than with online banking.

Consider the following carefully before choosing a password:

- Will it be protecting personal or business information (such as email and contacts)?
- Could someone accessing this account make financial transactions (such as through online banking or Internet auction houses)?
- Does access to this account provide access to other crucial data, such as credit card or banking numbers?

If you answered any of these questions with a "Yes", then you should definitely select the safest possible password. Also remember that many web applications send first-time passwords or "lost password resets" via email. A hacker who can gain control of your email account also automatically has access to those as well. You should therefore protect your email password extra carefully and change passwords immediately after receiving them via email.

The bottom line: Always think through the worst-case scenario if your password were to fall into the wrong hands – and then decide on an appropriate password strength based on that.

ONLINE SHOPPING

Books, electronics, clothes and even groceries – almost anything can be ordered online nowadays. The business is a boon for both sides. Buyers don't need to travel to the store, and often save money in the process. Sellers need only a warehouse, not a physical shop.

A SURVEY BY TELEKOM REVEALED THAT MORE THAN 80 PERCENT OF GERMAN INTERNET USERS ENJOY THE CONVENIENCE OF MAKING PURCHASES ONLINE.

WHAT SHOULD YOU KEEP IN MIND WHEN SHOPPING ONLINE?

Only trust businesses you know. In this spirit, when shopping online inform yourself about the store that you want to shop at. Customer evaluations and scores in forums can help you to avoid mistakes and be aware of damages.

When making online purchases, be sure that the login process and when entering personal data, at the latest, an "s" comes after the "http" in the address bar, such as **https://www.telekom.de** (German only). This shows that a secure connection has been made. You can recognize a secure connection by the lock symbol in the address bar of your browser.

Always enter a shop's address manually into your browser, or load the page from a previously stored bookmark. Do not follow links that you have received by email, as they could potentially lead to an insecure site. This prevents another chance for scammers to steal your data and password.

In any case, choose a secure password for your account with the store. More information about how to choose a secure password can be found under "Choosing a Safe Password".

Do not reveal your password to anyone! It should only be used when logging in to the shop. Harbor a healthy skepticism. A reputable shop would never ask for your login information via email or telephone. If you nevertheless receive a mail requesting this information, it is almost certainly a → **PHISHING** attack. More tips on protecting yourself against → **PHISHING** can be found under "Phishing".

Choose a secure payment method, such as bank transfer, invoice or COD. Or use an online payment service like ClickandBuy to pay for your purchase.

USING SMART-PHONES SAFELY

Keeping your private data on your Smartphone private and secure.

No question – Smartphones are the wave of the future. With ever-increasing sales numbers, they have also become a prime target for → TROJANS and other malware.

HOW TO STAY SAFE WHEN GOING MOBILE

The best software can't help you if it's gone out of date. Always be sure to install updates in a timely manner. That's easier if you only install applications that you really need. You can simply uninstall applications you don't need any more.

Keep the operating system on your device up to date as well. For iOS devices, you will be informed about available updates by a number on the "Settings" icon. For devices running the Android operating system, users must typically register with the device maker when they start the phone for the first time, and are then informed of updates thereafter. It's important that you register in this way, since new vulnerabilities in mobile operating systems – just like PC operating systems – are found all the time, and are sealed by security updates.

Do not install Apps (applications) from unknown sources. Watch out for hidden App costs, such as subscriptions or "in-app" purchases. For more information, see the chapter "Using Apps Safely".

THERE'S NOTHING MAGIC ABOUT BASIC PROTECTION

Protect your data against unauthorized access and your device against loss and theft.
You should always password-protect your smartphone and turn on the "Auto-lock" function for periods of inactivity. This prevents others from accessing your data, if taking your eyes off your device for a moment or if it goes missing. If your smartphone is lost or stolen, several manufacturers offer the option of tracking/tracing and a remote wipe of the device.

In this case of course routine backups of your data are all the more essential. Some smartphones offer the option of making a backup on the PC (such as iTunes for iOS devices).

In those situations it's important to have the device's SIM card blocked to prevent any additional costs from accruing. Inform yourself about which options (blocking, remote wipe, tracking, etc) are available for a given phone before making a purchase.

Also turning off various connection options like →**BLUETOOTH,** →**WLAN** and Near Field Communication (NFC), or even the mobile data connection if you're not actively using it, protects against hostile intrusions. This also conserves battery power.

If you don't want your smartphone to transmit your location, then you can turn off the location services function (such as GPS).

SECURITY À LA CARTE

Smarthphones work with various operating systems (Windows Phone, iOS, Android, BlackBerry OS or the new Firefox OS). The more widespread the system, the more attractive it becomes to attackers.

Set up your email account so that it uses →**SSL** or →**TLS** when sending or receiving emails. For more information on this, visit **http://www.e-mail-made-in-germany.de/** (German only).

Use the functions on your smartphone that encrypt your data and the memory card inside. Current iOS devices always encrypt the data. Access to the device should definitely be password protected. Current Android devices also offer optional encryption of the internal device storage. Inform yourself about the options offered by your device.

Do not store passwords, account numbers, → **PINS** and the like on your smartphone. There is also security software available for smartphones to protect against current threats off the Internet.

DELETING DATA ON OLD DEVICES

When buying a new cell phone, the question often arises: What should I do with my old device? Most end up in a drawer, or are given or sold to family members or friends. But what happens to the personal data on the old cell phone? Is it enough just to delete them? To ensure that strangers cannot restore your deleted data, the data should be completely removed by overwriting it. This is performed in different ways for different operating systems. For more information on how to permanently delete private information from your device, can be found under **http://www.telekom.com/dataprotection**. Be sure to also remove the storage card inserted into your smartphone. Delete all stored passwords. Remove the links to online shops and from Apps (emails, chats, Facetime).

If you want to shop on the Internet from a smartphone, be sure to read the tips in the chapters “Online Shopping” and “Phishing”.

USING APPS SAFELY

Applications – abbreviated as “Apps” – can do a lot: quickly tell you when the next subway train is coming, the current weather forecast, or giving you a game to play while you wait for the train. A few simple tips helping to use Apps more securely.

COMPARED WITH 2009, THE VOLUME OF MOBILE DATA TRAFFIC IN GERMANY HAS RISEN ALMOST FIVEFOLD ANNUALLY: FROM 34.9 MILLION GIGA-BYTES TO 170,1 MILLION GIGABYTES IN 2012.

WHAT DO YOU NEED TO CONSIDER WHEN USING APPS?

When installing an App in Android, you are shown which data that App can access. Because Apps often need to send and receive data, the right to make an Internet connection is usually top of the list. Some programs require significantly more access, however – for example to your telephone book, call log or location. Smartphones with the iOS operating system include a dedicated menu item ("Settings / Privacy") that gives the option to prevent specific handling of data, such as exporting location data. In many cases, though, the operating systems do not offer such options. The only options are then to either allow data to be forwarded or uninstall the software.

Problematic: Apps that receive full access to the address book (contacts). Most users keep not only telephone numbers, but also email addresses, birthdays and images of their friends and business partners here. In a worst case scenario, this data can be forwarded unnoticed to the App developer.

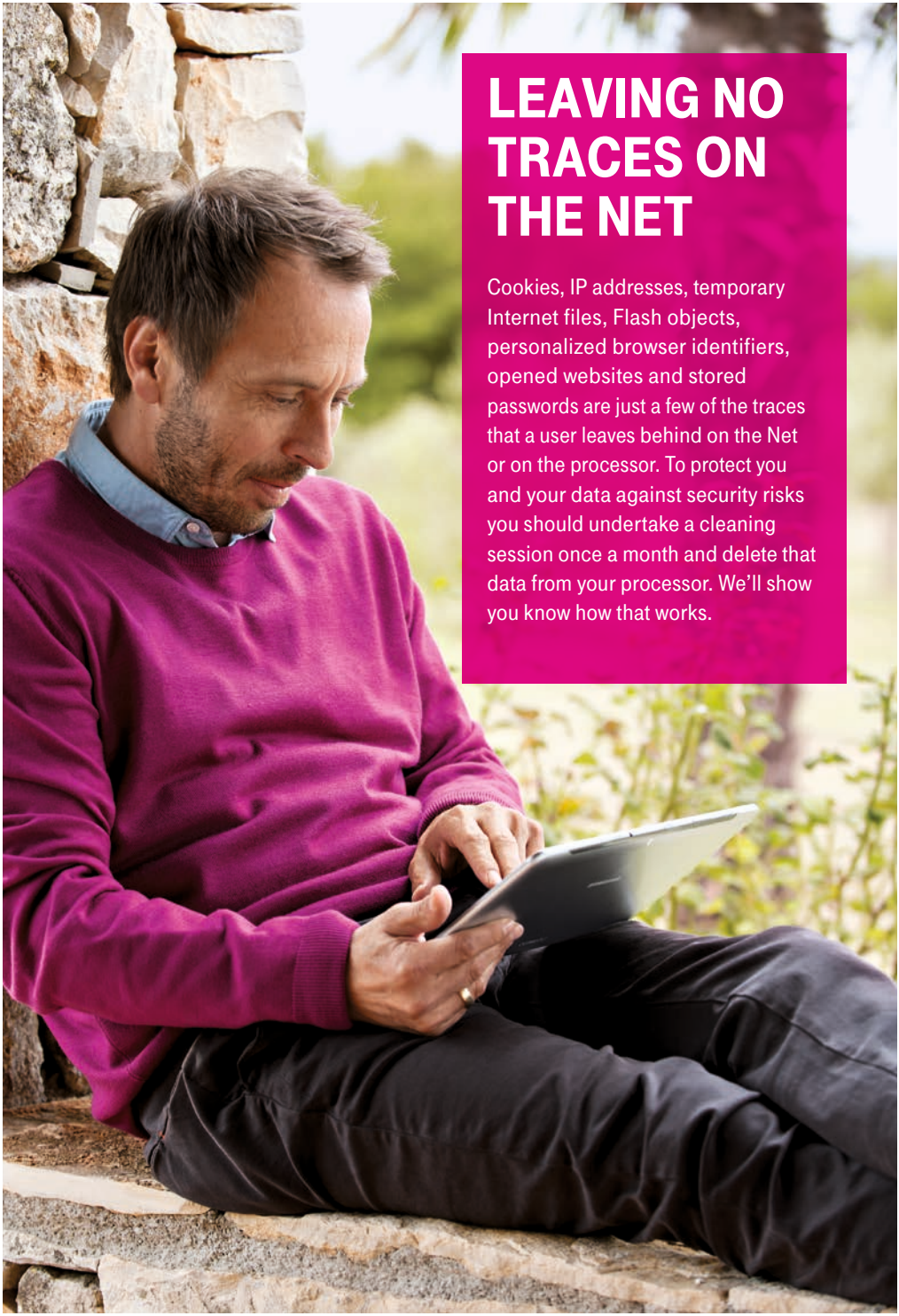
To be as safe as possible, read up on the corresponding App before installing it, especially as regards its privacy policy. Clear information should be provided on how the App handles your data. You can then decide whether you're prepared to accept the conditions of the developer.

If you find that your data is being processed in ways not indicated in either the user information or the system itself, then you should report this directly to the hotlines maintained by the App store's provider. An App that uses your smartphone as a flashlight doesn't need to access your address book or your current location. Most App stores have rules against secret data processing.

Only install Apps from a reliable source (such as Apple App Store or Google Play Store).

Watch out for hidden costs, such as subscriptions or "in-app" purchases.

Research how you can prevent in-app purchases before allowing anyone else to use your device. For some devices, authentication remains in place for a certain period after the purchase of an App. This could allow other persons to make a purchase at your expensive, without having to reenter a password.



LEAVING NO TRACES ON THE NET

Cookies, IP addresses, temporary Internet files, Flash objects, personalized browser identifiers, opened websites and stored passwords are just a few of the traces that a user leaves behind on the Net or on the processor. To protect you and your data against security risks you should undertake a cleaning session once a month and delete that data from your processor. We'll show you know how that works.

DELETE COOKIES

→ **COOKIES** are everywhere – entire Internet pages are built around them and won't function properly without them. → **COOKIES** are small files that are placed on your computer by an Internet page and contain information such as personal page settings, login information or unique user recognition. They can help to make surfing more comfortable. If you use the shopping cart function of an online shop, or change a website's language settings, → **COOKIES** are used. Yet → **COOKIES** can also be used to create a complete, personalized user profile. Besides HTML Cookies, there are Flash Cookies and Super-Cookies, with which information from a web site operator or advertiser are stored and later called-up. For whoever wants to prevent this, popular browsers like Internet Explorer, Firefox or Opera allow users to determine which → **COOKIES** are accepted and which not. Some browsers already offer an option for users to specify website operators and advertisers that they do not want to be tracked by. This function is based on the Do-Not-Track standardization initiative, supported by Deutsche Telekom and all current browser providers. For more information about blocking → **COOKIES** in your browser, please visit **http://www.telekom.com/dataprotection**.

Use different browsers.
Install browsers from different software makers and switch between them when visiting Internet sites. This leaves providers with different "fingerprints", preventing them from establishing a personal profile of yourself.

Switch between different search engines.
You leave behind traces on search engines as well. You can minimize these by using different search engines. Highly recommended is **https://ixquick.de/eng/** which complies with strict privacy policies. This way you have the opportunity to reach your search goal anonymously. Simply click on the "Proxy" option for your search results.

LITTLE HELPERS

It is not easy to find and delete all information as well as traffic and usage data. But there are programs to handle almost all of that work for you.

Spybot Search&Destroy
http://www.safer-networking.org/mirrors/
The →**MALWARE** protection program detects various forms of →**SPYWARE**, that try to sneak into the processor and spy on the user's surfing habits. The program deletes all usage data, including, including surf and download histories. It also seals up vulnerabilities in the browser and blocks potential entry points for attacks by malware and malicious websites.

Ccleaner
http://www.piriform.com/ccleaner/download/standard
The cleaning program attempts to remove superfluous and potential data leaks from the computer. It reviews, among others, the central Windows registry and directories where data like →**COOKIES** are typically stored.

WHAT CAN YOU DO IF INFORMATION ABOUT YOURSELF IS ON THE INTERNET, THAT YOU DON'T WANT?

Photos from your school days, from wild parties, from the last vacation or from the weekends: lots of people love sharing memories with friends on the social networks. But what can you do if you appear in the photos, but don't want the experience shared publicly?

And how could you find out what's out there about you on the Internet? A new Internet address is registered somewhere in the world every 1.5 to 2 seconds. With millions of websites in existence, it's virtually impossible to maintain an overview what information has been published.

https://www.secure.me/en/ is a service formed in cooperation with Deutsche Telekom AG to find, evaluate and delete unwanted information from Facebook. The program to review the online →**PRIVATE SPHERE** and online reputation is aimed at private persons, companies and families.

ANONYMOUS SURFING WITH IPV6

The introduction of the new IPv6 Internet standard will open the door to up to 340 sextillion new IP addresses – enough to give every conceivable

Internet-connected device around the world its own permanent IP address that would associate it clearly to one user. Deutsche Telekom has developed a solution to allow for anonymous surfing with the new IPv6 Internet standard. As a user you can decide the level of anonymity you desire as you search across the Net.

The new IPv6 addresses have two components: the so-called Network ID assigned by the network provider and the device-specific portion. The Telekom solution applies three steps to each of these portions:

Basic Protection

If your end device is connected to a Deutsche Telekom router with its network ID, then it is automatically assigned with the router's network ID. This is created randomly, and is factory preset for the routers.

Privacy Button

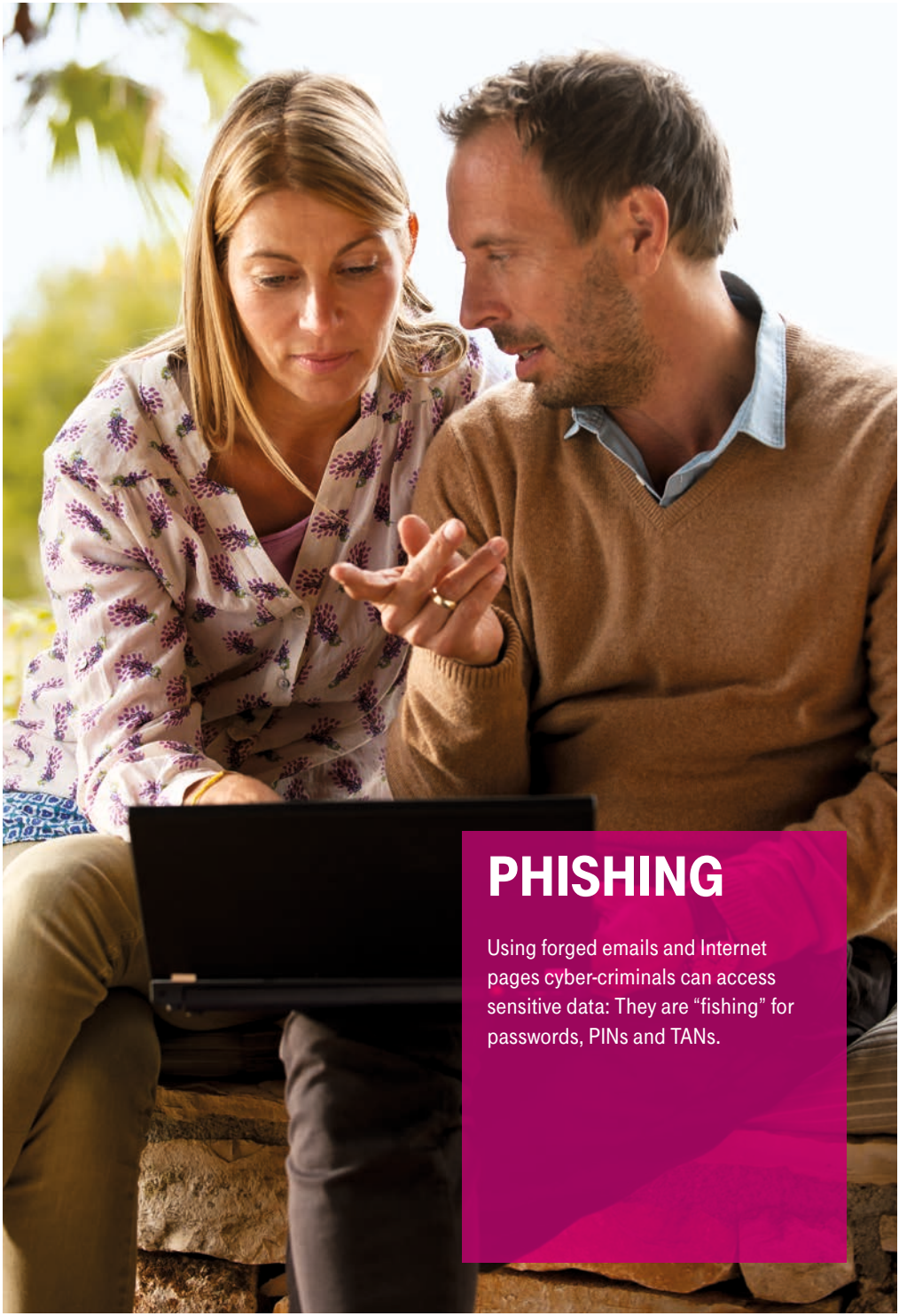
The website (firmware configuration for the router) of customer routers sold by Deutsche Telekom (Speedports) installs a so-called "privacy button", the symbol for privacy protections. Once activated, you'll receive yet another new address subsection for your network ID. This reassignment can be performed manually or automatically at a predetermined time.

Privacy Extension

Above and beyond this, most modern terminal devices automatically mask the second part of the IP address, the device portion, through a randomization process. Please always check that this function has been activated for your respective device.

TIP

When you first navigate to a website, review its privacy policy and General Terms & Conditions. This describes how the provider handles its data. If you are not agree with the policies listed there, then leave the site.



PHISHING

Using forged emails and Internet pages cyber-criminals can access sensitive data: They are “fishing” for passwords, PINs and TANs.

→PHISHING is an invented word that combines the words "Password" and "Fishing" to describe a method of fraudulently acquiring passwords, →PIN numbers and transaction numbers (→TAN). Through forged emails and websites that invite customers to enter their account data, including passwords, cyber-criminals gain access to sensitive data. The most frequent version uses a link to redirect the user to a realistic-looking but forged website for a bank or other company. In order to protect yourself against these attacks, follow these points:

PROTECTING AGAINST PHISHING ATTACKS

Pay attention to the companies with whom you do business. If the sender of the message is not one of those companies, then the email may well be fraudulent in origin, and is certainly spam.

Watch the subject line: Reputable banks and email providers will never send an email with a subject line like "Reviewing your Account URGENT" or the like.

You can expect from a company that provides services that they will know your name. Most →PHISHING emails are impersonal and, at best, address the reader with a formulation like "Dear Member", or "Dear Customer of XY Bank".

Service companies follow certain rules for communication. You bank will never request that you provide confidential data like →**PIN** or →**TAN** numbers in an email or telephone conversation. Exception: You have signed up for telephone banking with your bank and must provide your →**PIN** for authentication. Where uncertain, call your bank's publically listed number directly and query them.

Spelling and grammar mistakes in emails can occur even from reputable companies. If, however, mistakes are rampant in an email, your suspicious should be raised.

Incorrect or missing accents in the emails (such as ae instead of ä in German) are often a warning sign.

Just as suspicious, are requests to deactivate protective mechanisms like pop-up blockers and →**VIRUS SCANNERS**.

Always hover the mouse cursor over provided links and review the destination address shown in the status bar on the bottom of the page. This allows you to check whether the link actually leads to the desired site.

Activate your browser's →**PHISHING** functions. Various browsers come with this pre-installed, Firefox 3 and higher, Opera 9.5 and higher and Internet Explorer 7 and higher.

Whenever you need to enter personal data online, you should open a new browser window. Once the transaction is completed, it is best to log out immediately where possible and close the window.

WATCH OUT FOR PHISHING WEBSITES

Always be sure to look for the security certificate. This is indicated through the lock symbol on the address bar of your browser. If that lock is not present, then you are likely working with an insecure website.

If a secure connection is present, the abbreviation "https://" is shown in your browser's address bar. This encryption process prevents the data from being read or manipulated while you are working.

Be suspicious of unfamiliar security certificates! Certificates for banks and reputable online shops are familiar to standard browsers. Contact your bank or online shop before accepting new certificates.

Do not follow links to a bank's website, rather enter the address manually or use a bookmark. Links in emails often lead to forged but realistic-looking websites that try to trick you into revealing your data.

The login page for your bank will never request →**TAN** codes. If that is the case, please contact your bank immediately.

You can also use the address bar to determine the original domain name. The parts in the beginning are not important. For example: **www.firstnationalbankofplainville.financedepartment.randomISP.com**. You are not looking at a First National Bank of Plainville domain, but rather one hosted at randomISP.com.

ACTIVE STEPS AGAINST PHISHING

Phishing radar

To give consumers the chance to inform themselves about of the risks and put an end to fraud attempts quickly and unbureaucratically, the German Federal Ministry for Consumers and the Consumer Centre of Northrhine-Westphalia have created a →**PHISHING** radar at **http://www.verbraucherfinanzwissen.de** (German only). There you can post on a forum about →**PHISHING** emails, warn other users about the latest tricks, or send details about a →**PHISHING** email directly to the Consumer Central.

The best protection against Phishing mails: Delete them unread!

SOCIAL ENGINEERING

Scammers make targeted appeals to human sensibilities and weaknesses to gain access to confidential data.

WHAT IS SOCIAL ENGINEERING?

The goal of social engineering is to gain unauthorized access to private and sensitive data through interpersonal interaction. The criminals scout of their victim's personal situation, and assume a false identity..

HOW CAN YOU AVOID THIS?

Social engineering attacks are difficult to fend off, since the attacker is fundamentally exploiting positive human characteristics: the most important factor in fighting off social engineering attacks is thus a firm insistence on the part of the potential victim to clearly establish the identity and authorization of the caller on the phone or sender of an email before providing further information.

A simply query for the name and telephone number of a caller or a request to send your regards to a non-existent colleague can blow the cover of a poorly informed attacker. Even seemingly minor or useless information shouldn't be provided to unknown persons; as it could be used together with further information to circumvent a larger actual situation. It is important to issue a timely warning to all other potential victims. Your first point of contact should be the company's security department, as well as the contact address of the email provider and the person whose data was used in the forged identity.

The following points should be remembered:

- Always be mistrustful of any email where the identity of the sender is not firmly established.
- When called on the phone, do not provide even seemingly unimportant personal information to strangers, as it can be collated into useful information for further attacks.
- Do not ever reveal personal or financial data to email surveys, regardless of the apparent sender of the message.
- Do not provide personal data to sites reached via links provided in emails Enter the URL in your browser on your own.
- If you are uncertain about the identity of the sender of an email, make telephone contact to confirm the authenticity.

THE SAFETY BAROMETER

The Safety Barometer is a helpful tool for secure interaction with the Internet. It warns against new and recurring risks.

https://www.sicher-im-netz.de/pages/about-dsin (partly in English) displays a four-stage 'safety barometer' for the current hazard state:

Stage Green

Stage Green is designated as **"Normal Risk"** and indicates which protective measures the user should take to establish the greatest possible basic protection.

Stage Yellow

Stage Yellow is designated as **"Heightened Risk"** and warns against acute threats whose distribution or degree of damages however remains limited. Examples include small scale → **PHISHING** attacks.

Stage Orange

Stage Orange is designated as **"High Risk"** and is intended to warn users about significant dangers with significant penetration and/or degree of damage.

Stage Red

Stage Red is designated as an **"Internet Alarm"** and warns users about current threats, that endanger the availability or integrity of PCs and networks on a large scale.

Visit **http://www.t-online.de/sicherheit** (German only), the service page for Deutsche Telekom, for tips on how to protect yourself against potential threats. In times of normal risk level, when there are no acute warnings present, the barometer informs you on basic security measures and sensitizes you to current security-related themes and hazards.

SMART USE OF SOCIAL NETWORKS

Social Networks have become an important part of our daily life.
But what should you be aware of when using them?

Facebook, Google+, MySpace, StudiVZ, Xing and more: In an effort to stay in contact with friends, acquaintances and colleagues, many people reveal private data about themselves without a second thought on social networks.

The Internet is not a lawless place. Nevertheless not everyone follows the applicable rules, and not all countries have the same rules in the first place: data protection regulations intended to protect your right to control your own image or copyrights are often not taken seriously. This makes it all the more important that you carefully read through the General Terms and Conditions and Privacy Policy posted by the platform operator.

DESIGNING YOUR OWN PROFILE

First and foremost, as little personal data as possible – such as email addresses, telephone numbers, IM data, photos, etc – should be made public. After all, anyone revealing too many details about themselves makes it easier for →**PHISHING** attacks and spam mails to reach them.

Settings are available to restrict who can view your profile. The safest option is to allow access only to friends.

PRIVATE SPHERE

Learn more about each social network's settings regarding the →**PRIVATE SPHERE**. For more information about the best ways to protect your →**PRIVATE SPHERE** on different social networks, above and beyond the privacy policies and terms and conditions for each community, can also be found at **http://www.klicksafe.de/ueber-klicksafe/die-initiative/project-information-en/** (partly in English).

Personal data should only be made accessible to true friends.

Some networks offer the opportunity to divide friends into different groups, with each group assigned different access rights. This is a helpful way to control who can see which information.

PROFILE PHOTOS AND PHOTO ALBUMS

Even if it has come to seem normal to present yourself on the Internet using photos, some photos represent a real threat to your →**PRIVATE SPHERE**. Think through carefully beforehand which photos you'd like to appear on the Internet.

When creating a photo album, be sure to allow only friends direct access to that album. This is easily set in the album settings.

Only ever upload photos for which you hold the copyrights.

Photos that you've uploaded once to the Internet often remain captured in the →**CACHE** for a long time, even if you delete the photos or even the entire photo album (for more on this, visit **https://www.secure.me/en/**).

Because you'd never want to be shown in images that present you in a poor light, you should also respect the →**PRIVATE SPHERE** of friends and acquaintances and post images of them to the Net only after getting their permission first, and delete them upon request.

ADDING FRIENDS

Before accepting friend requests or sending such requests to others, check that you're certain who is on the other side.

MAKING APPOINTMENTS VIA THE INTERNET

Social networks are frequently used to set times to see friends or discuss other scheduling. Be careful never to divulge private information, including "I'm home alone today" on spaces that can be read by a wide audience. That kind of information should only be exchanged in private, such as via email or IM!

REPORT AND IGNORE FUNCTION

Persons, content or groups that violate the ethical standards of the network should be reported immediately. There is usually a Report button directly on your profile.

You can use the Ignore function to handle harassing users, preventing them from accessing your profile. This function also prevents them from sending you direct messages. You should also report these persons to their Internet Service Provider.

ADDRESS BOOK SYNCHRONIZATION

Many networks offer the option of connecting external email address books to the community. These pages then use that data to compare who is already a member of the community and who not (yet). What then happens with the data – and whether it is used for other purposes – is unclear.

IT'S NOT WHAT YOU SAY, BUT HOW YOU SAY IT

Back in the pre-Internet age, part of every proper education included reading and applying the etiquette found in "Miss Manners" and similar books. Good manners still exist in the age of digital communication as well: At **http://eetiquette.com/** you can find out more about virtual good behavior.

CLOUD COMPUTING

Data available everywhere, 24 / 7 – cloud computing makes it possible. Files that you store in online repositories, including the Media-center from Telekom, can be accessed on the Internet, regardless of the device.

OFF TO THE CLOUD – BUT SAFELY

→**CLOUD COMPUTING** means that files and programs are no longer stored locally. They are instead physically located on servers in the computing centers housed at the premises of the cloud service providers. The big benefit is that content and applications are available around the clock both at home and away from it on all Internet-ready devices. →**CLOUD COMPUTING** also brings some significant security concerns with it as well.

Choose a secure cloud service provider.
Don't trust your data to everyone. Research each provider and their services thoroughly. Telekom stores personal user files in the Mediacenter exclusively on servers located in Germany. As such they are subject to Germany's strict data protection regulations. Data transfer to the servers, which are protected with →**FIREWALLS**, is made using the latest encryption technology. The TÜV testing organization has already awarded a series of certificates for the service's adherence to the highest security standards.

Stick to the fundamental rules of secure IT usage.
In particularly: use only secure passwords and store them in a manner that is well protected from access by third parties. It's also important, that you change your passwords at regular intervals (see "Choosing a Safe Password").

GLOSSARY OF PRIVACY TERMS

→ **ANTI-SPYWARE** refers to programs that work to prevent spying on user data by malicious → **SPYWARE** programs.

→ **BLUETOOTH** is a method for networking two devices across short distances, using radio signals to exchange data.

→ **BOT NETS** are computer networks that are forged from individual computers that have been infected with malicious software. The Bot Net operator can remote control the "zombie" computers to send out spam emails and infect other processors.

→ **CACHE** is a commonly used term for the temporary storage space in a computer's memory. It automatically stores content viewed on the computer to make it quicker to return to the material a second time. All web browsers use a cache to speed up the process of display web sites. Major search engines also use caches to process Internet content.

→ **CLOUD COMPUTING** is an approach that stores data not (only) on one's own PC, but also on the remote servers of a service provider. The data can be available to authorized users at any time and from anywhere. The free Mediacenter from Deutsche Telekom is one example.

→ **COOKIES** are files, that are stored on the PC to ease the process of subsequent or repeated access to the same web server.

→ **FIREWALL** monitors the data flow on a network and secures the connection to and from the outside against unauthorized access. The firewall uses preset rules to check whether data packets, such as between the computer and Internet, should be sent.

→ **MALWARE** is an umbrella term for computer programs developed to execute programs unwanted by the user, including those that can potentially cause damages. The word is a combination of "malicious" and "software".

→ **PHISHING** refers to an attempt to use forged Internet addresses to gain access to an Internet user's data. The term is a combination of "Password" and "Fishing".

→ **PIN** stands for Personal Identification Number. This is a secret number or code of letters and numbers required to sign on to secure functions like online banking or to unlock a SIM card.

→ **PRIVATE SPHERE** is the non-public sphere, where a person has an unchallenged right to the free pursuit of their own interests without external influences. The right to privacy and the private sphere is considered a human right, and is anchored in the German Basic Law through what are known as "Personal Rights".

→ **SPYWARE** programs are snooping programs that try to spy on a user's information and data without the user's awareness. The data is then returned secretly to the program's maker. To prevent this spying, programs known as → **ANTI-SPYWARE** software are installed.

→ **SSL** or Secure Sockets Layer is the old designation for → **TLS** (Transport Layer Security). It is an encryption protocol for the secure transmission of data.

→ **TAN** is short for Transaction Number. It is a one-time password, primarily used in online banking, and most typically comprised of six numbers or a combination of numbers and letters. If a TAN is transmitted on a mobile device, such as via text message, that it is called a mobile TAN or mTAN.

→ **TLS** or Transport Layer Security, frequently referred by its old name → **SSL** (Secure Sockets Layer), is an encryption protocol for the secure transmission of data.

→ **TROJAN** is a computer program that tries to present itself as a utility or otherwise useful item. In the background, however, it typically carries out malicious programs without the user knowing.

→**VIRUSES** are computer programs that hide themselves in other computer programs, and replicate themselves there. Once started, this kind of program cannot be controlled by the user, and in fact itself often assumes control of the hardware, operating system or software. The designation as a "virus" refers to the way the program replicates itself – like an infection.

→**VIRUS SCANNERS** are programs that detect and block known computer viruses, →**TROJANS** and →**WORMS** an a processor, and then remove them.

→**WLAN** – Wireless Local Area Network. A WLAN connects one or more devices wirelessly with a base station. This creates a local network with data transmitted via radio. The WLAN base station typically contains a router than establishes a connection to the Internet.

→**WORMS** are malicious programs that infest computer networks. The worms rely on network services or user interactions to distribute. An example of communication channels of computer worms would be emails or software downloads off the Internet.

Stand 12/2013

CONTACT

Deutsche Telekom AG
Group Privacy
privacy@telekom.de

PUBLISHED BY

Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn
http://www.telekom.com/
dataprotection

LIFE IS FOR SHARING.