Guidebook on Cyber Threats:
Identifying and Combating Risks to Public and Private Sector Users and Citizens

By
Aleksandar Bratić

October 2022

DCAF Geneva Centre for Security Sector Governance

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF – Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Design & layout: DTP studio

This publication was developed within the framework of 'Good Governance in Cybersecurity in the Western Balkans', a DCAF – Geneva Centre for Security Sector Governance project, generously supported by the United Kingdom's Foreign, Commonwealth and Development Office.

DCAF Geneva Centre for Security Sector Governance

Contents

Executive summary

The world depends on connected digital systems and technologies for nearly all aspects of everyday life, in commerce, finance, communications, etc.

In this digital world, our personal data plays a central role. Hence, it is important to understand that personal data is both much more valuable and much more vulnerable than ever before.

It is not uncommon to hear of data breaches and cyberthreats that affect millions of users, even with most companies and institutions actively fighting to protect their data against hackers and cyber criminals. All of us play a role in securing cyber spaces, though. Cybersecurity is thus an imperative not only for large systems in organizations but for all of us, on our personal computers, mobile phones, and tablets.

A cyberthreat (or cybersecurity threat) is a malicious action intended to steal or damage data, or to disrupt individual systems or even an entire organization.

This guide will introduce various cyberthreats, which include a wide range of different kinds of attacks. The most common are:

- Social engineering attacks
- Phishing attacks
- Drive by downloads
- MITM attacks
- USB drop attacks
- Malware

Understanding these different cyberthreats will help you protect yourself, your personal data, and your systems.

Common cyberattacks

Social engineering attacks

In a social engineering attack, a target is misled and manipulated by an attacker into relinquishing personal data or access to their computer. This kind of attack relies on human interaction and usually involves the manipulation of a user so that they violate security procedures and best practices to gain unauthorized access to systems or share sensitive information.

Cybercriminals present themselves as trusted individuals to carry out social engineering attacks. The attack is then executed by tricking users into clicking malicious links or by physically gaining access to a computer.

Online Scams

There are various methodologies by which online scams, involving fraud by cybercriminals, are facilitated. Many are initiated through phishing emails, messages sent on social media or as SMS messages to mobile phones, fake tech support calls, and more. The purpose of these scams can range from credit card theft, to capturing user login and password credentials, to identity theft.[1]

Online scams succeed because they include elements realistic enough to make them appear credible, especially when a target is caught off guard. The cybercriminals who invent such scams are learning to take advantage of new technology, and it is their targets paying the price. To avoid becoming a victim of online scams, user must be very cautious about sharing personal data, and always:

- Avoid clicking on pop-up windows, or on links or attachments in texts or emails. Suspicious texts and emails should be deleted immediately.
- Know with whom you're communicating.
- Hang up immediately on any caller who asks for personal data or credit card details over the phone.

Phishing attacks

A majority of all cyberattacks begin with a phishing email. Phishing is a type of social engineering attack in which cybercriminals trick victims into handing over sensitive information or installing malware.

Even while technical security measures continue to improve, phishing remains one of the cheapest and easiest ways for cybercriminals to gain access to sensitive and personal information. Users merely have to click on a link and their security can be jeopardized to the extent that they may become victims of identity theft. Users can also compromise their personal information, login credentials (usernames and passwords), and financial information (credit card numbers) if they click the link.

How does phishing work?

Most phishing campaigns employ one of two basic methods:

- **Malicious attachments** in emails, which usually have alarming subject lines like 'INVOICE'. When opened, these attachments install malware on a user's machine.
- **Links to malicious websites** that are often clones of legitimate sites. Navigating to the site can trigger the download of malware, or the site's login page may contain credential-harvesting scripts.[2]

1 Online Scams, Avoiding Internet Scams, Norton, https://us.norton.com/internetsecurity-online-scams.html#

2 What is phishing? Everything you need to know, IT Governance UK

Types of phishing attacks

Spear Phishing

Spear phishing is a malicious email spoofing attack that targets a specific organization or individual, pursuing unauthorized access to sensitive information.[3] Spear phishing attempts are not likely to be executed by random attackers, but by cybercriminals seeking financial gain or other valuable information.

In a spear phishing attack, an email is sent from a reliable source but leads to a fake website mined with malware. These emails tend to use creative means to get the attention of users.

Spear phishing is much more efficient than other phishing attacks, but requires that cybercriminals spend time and resources working on pre-attack research, as they will be more successful if they learn about their target before launching an attack.

Whale Phishing / Whaling

Whale phishing is similar to spear phishing, with a few notable differences. Whereas spear phishing is usually directed at members of a group, whale phishing is focused on a specific individual – usually the 'biggest fish' at the target organization or an individual with noteworthy wealth or power.

Vishing

Vishing, or "voice phishing", involves the manipulation of people over the phone. Attackers seduce a target to reveal sensitive information in an attempt to use this data for their own benefit, typically to gain financially.

Smishing

The term smishing refers to SMS phishing, and involves a text message rather than an email. Targets generally receive a misleading text message that compels them to provide personal or financial information to cybercriminals pretending to be a government agency, bank, or other legitimate company.

Smishing attackers often seek personal or bank account information, such as account credentials, credit card numbers, and identification numbers. Then, they use that information to carry out various attacks, including financial, gift, or customer support fraud.

Drive-by downloads

In a drive-by download attack, downloads of malicious script end up on a computer or other device without the user's knowledge, exposing the user to various cyberthreats. This can happen on any device running any operating system and usually occurs when a user navigates to and browses a compromised website.

Man in the middle (MITM) attacks

An MITM attack takes place when a cybercriminal secretly inserts themselves between devices, or between a device and an insecure wi-fi network, to intercept communications that may then be read and/or modified. In such a case, a user can unintentionally pass credentials or other information to the cybercriminal.

3 What is Phishing?, gfidigital.com

USB drop attack

In a USB drop attack, a USB device containing malicious code is plugged into a computer.

Typically, the cyberthreat posed by this kind of attack is malware or virus infection. Infection through a USB drive can be both intentional and unintentional, depending on the malware in question.

It is wise to stop trusting obsolete USB technology, and embrace the power of secured digital networks by using cloud storage.

Malware

Malware is a general term used to define any file or program intended to harm or disrupt a computer. This includes:

- **Botnet software** designed to infect large numbers of devices connected to the internet. Some botnets comprise many devices, each using a relatively small amount of processing power. This can make it difficult to detect this type of malware, even when the botnet is running.
- **Ransomware attacks**, which encrypt user information and require payment in return for the decryption key, to retrieve the information. Paying a ransom does not necessarily guarantee recovery of the encrypted data, though.
- **Spyware** used to illicitly monitor a user's computer activity and harvest personal data.
- **Trojans** that appear as legitimate software but perform malicious activity when executed.
- **Viruses and worms**, which are malicious code installed without the user's knowledge. Viruses can replicate and spread to other computers by attaching themselves to other computer files.

Worms are also self-replicating, but do not need to attach themselves to another program to do this.[4]

4 Types of Cyber Threat in 2019, IT Governance USA

How to stay safe online

Handle personal data and your digital identity with care

As individuals, we identify and categorize ourselves in many ways, using our name, address, age, profession, and more. Our identity is also represented in many forms, from driver's licenses, to social security cards, to birth certificates, to work and school security badges.

Considering all these different forms of identity at use in our daily routines, both online and offline, it is unavoidable that much of our private data exists in cyber and other spaces, and is very likely being used without our consent. We simply have no idea how much of that data is stored in locations we never intended it to reach, and could be accessed and exploited by people we don't know.

It is obvious that things like passwords, banking details, and personal data should never be shared, but even information about close relations or the name of your pet could be used by cybercriminals to compromise your security. These personalized facts may help them answer security questions meant to protect your accounts, or offer hints that lead them to your password(s). It is smart to assume that hackers are constantly searching for ways to exploit your personal data.

Identity theft and data breaches are major threats for a number of reasons, but perhaps primarily because they compromise our sense of self, as identity is fundamental to how we interact in the world. Thus, to re-take control of your personal data:

- Do not use personal data in usernames or passwords associated with online accounts
- Do not share personal data to earn discounts in online shops
- Do not share unnecessary private information on social media
- Always verify how your personal data will be used and secured in applications
- Always verify that a website is secure (https vs http) before providing personal data
- Be cautious of any service offered for free, for which you may be "paying" unknowingly with your data

Use complex passwords

Always use complex passwords that do not contain: obvious and easy to guess number combinations (such as 12345, 111111, 123321, etc.), popular names, or strings of letters formed from a horizontal or vertical line on a QWERTY keyboard (such as asdfghjkl, qazwsx, 2wsx, etc.).

Surprisingly, the most generic password – "password" – remains very popular! If you are using this as a password, change it NOW.

Here are some tips to creating a secure password:

- Use at least 15 characters, and more if possible
- Mix up letters (both lowercase and uppercase), numbers, and symbols
- Never use sequences of numbers or letters (such as "qwerty")
- Avoid substitutions, as in "Ra!nb0w5", where letters in a common word are simply replaced by similar-looking numbers and symbols

Use different passwords for different accounts. This way, even if one account is compromised, others are not at risk.

Remembering passwords, especially the kind of complex passwords recommended here, can be a challenge. However, this can be solved by using a password manager. It is advisable to use only reputable password managers such as LastPass or 1Password.[5]

Double-check links before clicking

Be sure to know and trust links before clicking on them in emails or visiting websites.

One way to determine if a link is safe is to mouse over it, without clicking. This will show a preview of the full link in the status bar of a web browser, allowing a user to verify that the link matches information in the email and navigates to the page identified. It is also smart to verify the correct link by searching for it independently, based on information in the email.

If an email includes instructions to log in, it is always safer to navigate to the official site in question and sign in there, rather than clicking the login link provided in the email. This is true even of links sent by friends on social network applications.

If an email or site requests that you log in to your bank or other sensitive accounts, it is always wise to call and verify the request with that institution.

Always think twice before clicking on downloads. Some cybercriminals aim to infect devices with malware by tricking users into downloading compromised applications and other software. Before downloading, take care to ensure that the site or application associated with the download link is legitimate, and avoid downloading anything that appears suspicious.

Use secure wi-fi networks

Unless it is simply unavoidable, never use unsecured or unlocked wi-fi networks that lack password protection. If this cannot be avoided, do not log into any online accounts or apps while connected, and never share any personal or financial information online.

Cybercriminals often set up fake wi-fi hotspots to bait unsuspecting users. Once someone logs in to these networks on their phone, a cybercriminal can see almost everything they do. To ensure that the wi-fi connection you use in public is not a hotspot created for these nefarious purposes, it is usually easiest to ask an employee of any business or company for the name of their wi-fi network.

Also, devices should not be set to automatically connect to wi-fi networks, other than at work or home. Always set devices to ask before connecting, so that you are aware when and to what networks they connect.

Use a VPN

A VPN, or virtual private network, provides a secure connection for your devices to the internet, preventing bad actors from monitoring your activity or accessing your information. A VPN can be a good way to secure a wi-fi connection at home, and while out in public using unsecured wi-fi.

The only drawback to the enhanced security of VPNs is that they can lead to slower internet connection speeds. This is because a VPN routs data through another server to secure it.

As more people work from home, one way to stay protected is to use a VPN (and keep it updated).

5 Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Use sites that are preceded by https://

The “s” in https:// stands for “secure” and indicates that any data entered on a site preceded by this prefix will be encrypted. Hence, when logging into any site, you should always check that the address (in the web browser address bar) begins with https:// and not http://. You may also see a padlock symbol next to the web address, indicating that the site is secure.

When shopping online and providing personal data such as bank account or credit card information, always double-check that the website to which you have navigated is secure.

Turn your Bluetooth off

Bluetooth communications can be compromised and even manipulated without a user’s knowledge. This does not mean you should never use Bluetooth to pair devices, but it is best to turn it off when it is not actively in use.

Install antivirus and antimalware software

It is simply not advisable to surf the web without any protection from viruses and malware. Even free and low-cost antivirus software can be effective if you choose carefully and wisely, but spending a little on this software may be worth it to better guarantee you can avoid the headache of dealing with malware or ransomware.

If you already use antivirus or antimalware software, make sure you keep it up to date!

Antivirus and antimalware software that is widely recommended includes:

- Microsoft Defender (this comes preinstalled with the Windows OS and just needs to be turned on and updated)
- Norton AntiVirus Plus
- Bitdefender
- AVG
- Malwarebytes
- Avast
- SpyBot Search and Destroy

Backup your data

Our computers and other devices host all our important data, but if these devices are compromised, damaged, lost, or stolen, this important data may be lost. Whether this loss is due to hardware failure, theft, natural disaster, or infection by malware, it can be expensive or impossible to recover data.

Thus, a backup – **a digital copy of your most important information** – is crucially important. When you back up data, copies of your files (photos, documents, videos, etc.) are saved to an external storage device or online cloud service. This means you can restore your files if something goes wrong. We recommend backing up regularly.[6]

6 Back Up and Restore - Microsoft Windows, Cyber.gov.au

There are several ways to back up data. Here are the strengths and weaknesses of each:

- **Back up to an external drive**: This can be initiated by using the built-in backup features on most computers, either by periodically connecting the drive to the computer and using the backup tool or by leaving it plugged in for automatic backups on a schedule.
  Pros: Cheap and fast
  Cons: External drives can be lost or stolen, and can break down over time
- **Back up data on your computer**: Depending on the device and operating system, there are different ways to back up data on a computer. For example, iCloud is available to users of iOS devices; Time Machine to Mac users; and different tools in different versions of Windows (8.1, 10, and 11, etc.) to PC users.
  Pros: Cheap and fast
  Cons: Backup can be lost or stolen
- **Back up to a cloud storage service**: Backups can be stored in the "cloud" with a service such as Dropbox, Google Drive, Microsoft OneDrive, or similar. This allows you to automatically synchronized backups with other devices, and means that if your computer does not function or is stolen, you will nonetheless have copies of all the files backed up online.
  Pros: Easy, fast, in many cases free, and the best protection against all types of data loss
  Cons: Most cloud services offer only a few gigabytes of storage space for free, and most people will find it necessary to pay for extra storage in order to back up all their files[7]

It is worth considering where your most important data is hosted and ensuring that multiple copies of it are saved at all times. Ideally, those copies should exist in more than one physical location.

7 Best ways to back up your computer, Nerds in a Flash

Conclusion

As the cyberthreat landscape grows more complex and cybercriminals take advantage of emerging technologies and trends, including social media, remote workplaces, and our dependence on smartphones, it is more essential than ever that users understand how to stay safe in cyber spaces. The best approach is to implement the recommendations in this guidebook, which outline smart behaviours and recommend various tools. Ultimately, staying safe online requires a balance of preparation, prevention, and awareness. You can avoid being victimized, or at least avoid the worst outcomes from cybersecurity events, if you prepare for data loss by backing up files, prevent data breaches by installing appropriate tools, and keep aware of the kinds of attacks favoured by cybercriminals.

References

Online Scams, Avoiding Internet Scams, Norton

What is phishing? Everything you need to know, IT Governance UK

What is Phishing?, gfidigital.com

Types of Cyber Threat in 2019, IT Governance USA

What Is Cyberbullying, StopBullying.gov

Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Back Up and Restore - Microsoft Windows, Cyber.gov.au

Best ways to back up your computer, Nerds in a Flash

Annex: Good practices checklist

COMMON CYBERATTACKS	
SOCIAL ENGINEERING	- In social engineering attacks, a target is misled and manipulated by an attacker into relinquishing personal data or access to their computer(s). These attacks rely on human interaction and usually involve the manipulation of a user so that they violate security procedures and best practices to gain unauthorized access to systems or share sensitive information.
PHISHING ATTACKS	- Phishing is a type of social engineering attack in which cybercriminals trick victims into handing over sensitive information or installing malware. These attacks can take different forms: • Spear Phishing – a malicious email targets a specific organization or individual, pursuing unauthorized access to sensitive information. • Whale Phishing/Whaling – an attack focused on a specific individual, usually the "biggest fish" at the target organization or an individual with noteworthy wealth or power. • Vishing – an attempt to obtain a victim's personal data and use it to gain financially by manipulating a target over the phone. • Smishing – a misleading SMS message meant to compel the recipient to provide personal or financial information (account credentials, credit card numbers, etc.), sent by cybercriminals pretending to be a government agency, bank, or other legitimate company.
DRIVE-BY DOWNLOADS	- In a drive-by download attack, a user unintentionally and unknowingly downloads malicious script on to a computer or other device by navigating to or browsing compromised websites, exposing the user to various cyberthreats.
MAN IN THE MIDDLE (MITM) ATTACKS	- MITM attacks occur when a cybercriminal secretly inserts themselves between devices, or between a device and an insecure wi-fi network, to intercept communications that may then be read and/or modified. This can lead to a user unintentionally passing credentials or other information to the cybercriminal.
USB DROP ATTACK	- In a USB drop attack, a USB device containing malicious code is plugged into a computer.
MALWARE	- **Botnet software**: infects large numbers of devices connected to the internet. - **Ransomware attack**: encrypts user information, then requires payment in return for the decryption key needed to retrieve it. - **Spyware**: a form of malware used to illicitly monitor a user's computer activity and harvest personal information. - **Trojan**: a type of malware that hides as legitimate software but performs malicious activity when executed. - **Viruses and worms**: malicious code installed without a user's knowledge. Viruses can replicate and spread to other computers by attaching themselves to other computer files. Worms are also self-replicating, but do not need to attach themselves to another program to do this.

HOW TO STAY SAFE ONLINE	
NEVER SHARE PERSONAL INFORMATION	- **Never share, online or in person:** • passwords • banking details • personal data - **To re-take control of your personal data:** • Do not use personal data in usernames or passwords associated with online accounts • Do not share personal data to earn discounts in online shops • Do not share unnecessary private information on social media • Always verify how your personal data will be used and secured in applications • Always verify that a website is secure (https vs http) before providing personal data • Be cautious of any service offered for free, for which you may be "paying" unknowingly with your data
CREATE AND USE COMPLEX PASSWORDS	- **Always use complex passwords that:** • are at least 15 characters long (longer, if possible); • mix up letters (both lowercase and uppercase), numbers, and symbols; • never use universal sequences of numbers or letters (such as "qwerty"); and • avoid substitutions – as in "Ra!nb0w5" – where letters in a common word are simply replaced by similar-looking numbers and symbols. - **Use different passwords for different accounts** - **Consider using a password manager**
DOUBLE-CHECK LINKS BEFORE CLICKING	- **When reading email or visiting websites, users should always know and trust links before clicking on them**. **To avoid clicking on malicious links**: • Mouse over links to see a link preview, and verify that it matches information in an email or shows the expected website or webpage • If an email includes a log-in link, it is safer not to click the link provided in the email but to go instead to the official site for the relevant organization/company and sign in there. • If an email or site requests a user log into bank or other accounts, always call to verify the request. • Before downloading from any website, take care to check the legitimacy of the site, and always avoid downloading anything that appears suspicious for any reason.
USE SECURE WI-FI NETWORKS	- Never use unsecured or unlocked wi-fi networks (with no password), unless it is unavoidable. - When using an open wi-fi network, avoid logging into any accounts online or entering any personal or financial information into apps - Set up devices so that they do not automatically connect to wi-fi networks
USE A VPN	- A virtual private network, or VPN, provides a secure connection to the internet and prevents bad actors from monitoring your activity or accessing your personal information - There are many VPN providers, and a VPN must be downloaded, installed, and connected to a server.
USE SECURE SITES (HTTPS)	- When logging in online, the URL in the browser's address bar should begin with https://, not http:// (the "s" means "secure"). - There may also be a padlock symbol shown next to secure website addresses.
TURN OFF BLUETOOTH	- If you sometimes connect to devices through Bluetooth, be sure to turn it off when it is not actively in use, to avoid being compromised or even manipulated.
USE ANTIVIRUS AND ANTIMALWARE SOFTWARE	- Even free and low-cost antivirus and antimalware software can help protect users from malware or ransomware. Be sure to keep antivirus and antimalware software up to date!
BACKUP DATA	- When data is backed up, copies of files (e.g., photos, documents, videos, etc.) are saved to an external storage device or an online cloud service. - This digital copy of data can help restore a system if it is compromised, so it is important to back up regularly

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva