U.S. Embassy in Romania

Romanian Association for
Information Security Assurance (RAISA)

National Association for
Information Systems Security (ANSSI)

Romanian National Computer Security
Incident Response Team (CERT-RO)

CYBERSECURITY GUIDE

ISBN: 978-973-0-33645-0

PROGRAM TITLE:

Enhance Cyber Capacity Building in Romania for
Preventing and Combating the Cybercrime Phenomenon

PURPOSE OF THE PROGRAM:

The program goal is to strengthen the cyber capacity in Romania by
raising cybersecurity awareness and improve the skills of
criminal justice authorities and private sector in fighting cybercrime.

U.S. Embassy in Romania

Romanian Association for Information Security Assurance (RAISA)

A project developed by the Romanian Association for Information Security Assurance (RAISA).
This project was funded in part by a grant from the United States Department of State.
The opinions, findings and conclusions stated herein are those of the author[s]
and do not necessarily reflect those of the United States Department of State.

eBook: Cybersecurity Guide

Authors: Iulian ALECU, Costel CIUCHI, Toma CÎMPEANU, Iulian COMAN, Larisa GĂBUDEANU,
Ioan-Cosmin MIHAI, Cosmina MOGHIOR, Nelu MUNTEANU, Gabriel PETRICĂ, Ionuț STOICA, Cătălin ZETU

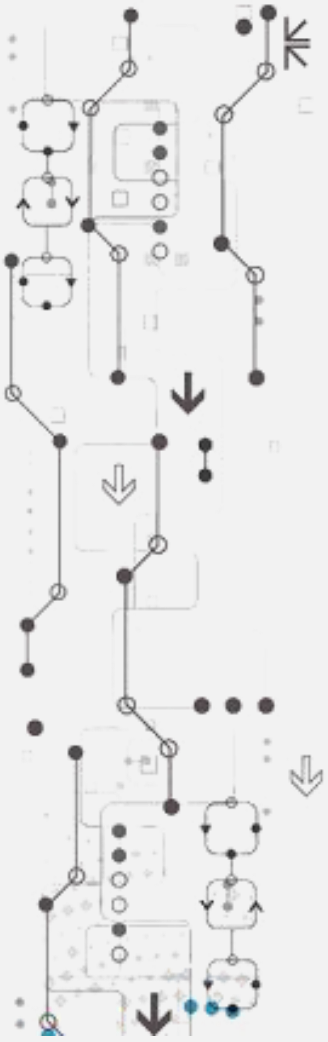
Version: 1.1

Website: www.cyberlearning.ro/cybersecurity-guide/

ISBN: 978-973-0-33645-0

DOI: 10.19107/CYBERSEC.2021.EN

CONTENTS



ABOUT THIS GUIDE

DAN CÎMPEAN

General Director of the Romanian National Computer Security Incident Response Team (CERT-RO)

We play a sometimes-involuntary role in an unrivaled, accelerated digital transformation on a personal, social and economic level. Subsequently, we perceive that each individual is urged to acquire new skills, to expand their knowledge, to shift their cultural perspective.

Just as, during our childhoods, we learned the alphabet with our first-grade teachers' assistance and broadened our horizons of knowledge, facilitated by the love and dedication of educators, today we will have to resume the accumulation of a new elementary set of learnings. This time we'll be guided by cybersecurity experts towards the acquisition of a complex, sophisticated, exciting body of knowledge, deeply technological yet indispensable for the 21st century.

It is imperative to have active promoters for cybersecurity concepts, education programs and awareness. It is essential to be able to find practical and effective ways of comprehensively promoting "cyber hygiene" and additional preventive measures at the national level, that should be transmitted to and regularly applied by citizens, organizations, and economic operators, in order to minimize their exposure to cyber-risks.

And now we have good news to share...

Written in the form of a concise and pragmatic cybersecurity guide, this superb work epitomizes, in just a few dozen pages, over a century of concrete experience from its 11 authors.

Basic concepts such as confidentiality, integrity, availability, personal data protection, but also specific elements from European or Romanian legislation related to the cybersecurity field, are transmitted in a clear, simple, but not simplified form.

I dare say that this guide is one of the much-needed publications for all of us, today. Moreover, I am convinced that it will contribute concretely and effectively to educating the general public, in order to improve the overall status of cybersecurity in Romania and the protection of Internet users' personal data, through the invaluable help it offers readers with understanding, preventing and countering risks, threats and vulnerabilities in cyberspace, or those related to technologies we use on a daily basis.

On behalf of the countless people, experienced or otherwise, who will make use of this guide's recommendations in practice, I would like to share with our authors, in recognition of their educational and awareness work, a short message used in the world of ethical hackers: RESPEKT!

SECURE YOUR PC / LAPTOP

Securing workstations (PCs, laptops) and other devices connected to wired or wireless networks is an essential condition both for ensuring the confidentiality and authenticity of sensitive data, but also for carrying out normal activities at the level of regular users.

HOW TO PROTECT

1 SECURITY TOOLS AND SUITES

It is recommended to install anti-malware applications or high-performance security suites to ensure protection against the latest types of cyber threats (e.g. ransomware or trojans). Permanently updating the database with malware signatures is a mandatory condition for detecting the latest types of threats.

2 SENSITIVE DATA ENCRYPTION

It is recommended to use third-party applications or operating systems that have implemented facilities for encrypting sensitive data (within files, folders, or an entire drive).

3 SECURE OPERATING SYSTEM

It is achieved both by fixing security breaches and software bugs in all components of the operating system (by applying available updates, automatic or manual) and by controlling user access to computer resources (permissions, access to files, services, and applications).

4 UPDATE APPLICATIONS

It is a necessary action because it prevents some cyber-attacks and costly data leaks, helping to keep safe sensitive data. Users must activate the automatic update function of any essential application (within the operating system or antivirus, firewall, and IDPS).

5 BACKUP DATA

Data must be periodically saved on reliable magneto-optical media, stored in secure locations and (possible) encrypted to prevent unauthorized access. These copies must be kept in multiple physical locations to avoid both natural disasters and internal threats within the company.

6 PASSWORD MANAGEMENT

Sometimes it may be advisable to use passwords manager tools to store unique, computer-generated passwords.

The passwords have to be strong (many alphanumeric characters and special symbols), not reused on multiple accounts and changed periodically.

7 TWO-FACTOR AUTHENTICATION

Using two-factor authentication is a very effective and modern method, which uses an additional device (such as a security token or smartphone) to confirm in a further step the identity of the person authenticating. Also, authentication based on biometric data must be considered.

8 USE RESTRICTED ACCOUNTS

The use of accounts with limited access rights instead of an administrator account will deny access to sensitive areas of the operating system and will naturally block the attacks against OS services, files, or libraries.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

SECURE YOUR MOBILE DEVICE

In the last decade, mobile equipment (smartphones, tablets) has experienced an exponential degree of development and use. In this context, ensuring the security of this equipment, essential in communication and online services, is a key objective.

HOW TO PROTECT

1 *ACTIVATE ANTI-THEFT PROTECTION FUNCTIONS*

Some useful functions can be activated:

- Facial or fingerprint recognition.
- Unlock device by patterns or by PIN.
- Equipment localization.
- Blocking access or deleting data remotely.

2 *SYNCHRONIZE DATA*

Synchronizing data with other equipment or using cloud services allows important information (contacts, SMS, documents, or pictures) to be available when the equipment is lost or stolen.

3 *UPDATE THE APPLICATIONS*

The operating system and applications need to be constantly updated to fix security breaches and use the latest features.

4 *DISABLE UNUSED CONNECTIONS*

Is recommended to disable infrared, Bluetooth, or Wi-Fi connection if it is not in use, to block an unauthorized access.

5 *USE SAFE APPLICATIONS*

Is recommended to download applications only from official sources and to disable the option regarding the download of unsafe applications.

6 *USE CLEAN STORAGE MEDIA*

Before connecting to mobile device, the removable storage media must be scanned with antimalware tools.

7 *SHARE PERSONAL INFORMATION*

Sharing personal information such as real-time geographical location (using GPS or wireless networks) can allow third parties to monitor the usual routes and daily activities.

8 *USE QR CODES CAREFULLY*

QR (Quick Response) codes may contain links to malicious web pages with various harmful effects regarding data security: activation of the camera/microphone, extraction of geo location, access to files, contacts, or SMS, sending unwanted messages via e-mail, SMS, or chat applications, launching DoS packages, or identity theft.

9 *APPLICATION PERMISSIONS*

Use Permission Manager to set application access to various resources (camera, microphone, location, storage, etc.).

10 *EXTRA SECURITY FOR BUSINESS DEVICES*

The equipment provided by organizations and used during travels must be secured regarding the encryption of data, wireless connections (Bluetooth, Wi-Fi) or removable media (USB drives, CDs / DVDs external hard disks, etc.).

11 *USE SECURE DATA CONNECTIONS*

It's recommended to avoid public Wi-Fi hotspots for connecting to Internet and use instead mobile data whenever is possible.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

SECURE YOUR NETWORK

An effective security of your home network can be achieved by implementing the following recommendations regarding technical aspects, security policies, employees training, or awareness activities.

HOW TO PROTECT

1 PHYSICAL SECURITY

It refers to access control in the areas protected by video surveillance, security personnel, or blocking access (barriers, locks, doors), securing the servers and cable trays.

2 FIREWALL, INTERNET PREVENTION AND DETECTION SYSTEMS

Are useful components of the IT infrastructure in any organization, for monitoring the network and tracking malicious activities (detecting intrusions, blocking malware or filtering dangerous content).

3 VIRTUAL PRIVATE NETWORK (VPN)

VPN technologies are solutions for secure remote access and encryption of information. It is recommended to be implemented when sensitive data is transferred through the Internet.

4 USE PRINCIPLE OF LEAST PRIVILEGE

Each new account must have allocated the most restrictive access rights, and other access rights will be added as needed. When access to sensitive data is no longer required, all appropriate privileges must be revoked.

5 MONITOR THE USERS

To minimize the risks of an insider attack, it is necessary to limit the number of privileged accounts and grant minimum permissions. Any privileged account must be deactivated if it is no longer justified to keep it.

6 SECURITY MEASURES FOR WIRELESS NETWORKS

- Use secure network protocols (e.g., WPA2) and compatible equipment.
- Disable unused services and functions.
- Filter accepted equipment in the network by the MAC address.
- Hide network SSID.
- Assign static IP addresses or reduce the range of dynamically allocated IP addresses.

7 CHANGE THE DEFAULT PASSWORDS FOR NETWORK EQUIPMENT AND IoT DEVICES

Because many devices have the default settings published on Internet, to avoid misappropriation for malicious purposes, the default settings must be changed immediately.

8 TRACK THE ACCESS OF THIRD PARTIES TO DATA

Monitoring the third parties access to data would allow the detection of harmful activities and investigations can be initiated when necessary.

9 INCREASE USER AWARENESS

It can be achieved by informing the organization's employees about the reasons and effects of security measures. The proper training of employees will lead to an increased cybersecurity level in organizations.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

MALWARE

The malware (malicious software) is an application or script intentionally designed to cause damage to data, computers or networks.

The main types of malware:

- **Viruses:** replicate themselves by modifying other computer programs and inserting their own code.
- **Trojans**: give the impression of doing legitimate operations, when they actually try to explore the system vulnerabilities and to allow cybercriminals to illegally access the system.
- **Worms**: apps with destructive effects infecting the computer system and propagating through the Internet.
- **Ransomware:** encrypt or block the access to the files and ask for a ransom in order to remove the restriction.
- **Cryptominers**: use computer resources to mine cryptocurrencies for cybercriminals.
- **Adware:** transmit aggressively advertisement to the user.
- **Spyware**: capture various information about the user's activity on the Internet.
- **Rogueware:** mislead users to pay for removing false infections detected in the operating system.

HOW TO PROTECT

1. ***INSTALL AN ANTIVIRUS SOLUTION*** to detect and remove the malware in real time.
2. ***INSTALL A FIREWALL APPLICATION*** to inspect the traffic from websites, e-mails and applications.
3. ***UPDATE THE OPERATING SYSTEMS AND THE APPLICATIONS*** to patch the existent vulnerabilities.
4. ***DISABLE AUTOMATIC EXECUTION OF CODE ON WEBSITES*** to prevent the installation of file-less malware.
5. ***USE E-MAIL FILTERING*** to recognize and detect the malicious emails and attachments.
6. ***AVOID USING ADMIN ACCOUNTS*** to prevent malware to have administrator privileges.
7. ***BACKUP YOUR DATA*** to restore it in case of a successful infection with malware.
8. ***USE ADVANCED TOOLS***, for malware detection and mitigation, like *Intrusion Detection and Prevention Systems (IDPS).*
9. ***MONITOR THE LOGS*** using *Security Incident and Event Management (SIEM)* solution.
10. ***USE SECURITY POLICIES*** that specify the steps to be followed in case of infection.
11. ***REDUCE ACCESS TO POWERSHELL*** functions, to limit the malware to execute malicious code into the console.
12. ***REPORT THE SECURITY INCIDENTS*** to the National Computer Security Incident Response Team.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

E-MAIL BASED ATTACKS

This types of attacks usually appear to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL. Although the mechanisms of e-mail based attacks vary, the objective is almost always the same: steal money or data.

Types of e-mail attacks:

- **E-mail bombing:** repeatedly sending an e-mail with large files attached, to a specific e-mail address. This attack leads to available space filling on the server, making your email account inaccessible.
- **E-mail spoofing**: sending e-mails with the sender's address modified. This attack is used to hide the real identity of the sender to find out confidential details or the data needed to access an account.
- **E-mail spamming**: sending unsolicited e-mails with commercial content. The purpose of these attacks is to attract the e-mails recipients to access some websites and buy more or less legitimate products or services.
- **E-mail phishing**: sending messages to determine the recipients of e-mails to provide information on bank accounts, credit cards, passwords, or other personal details.

HOW TO PROTECT

1. ***DISABLE AUTOMATIC EXECUTION OF CODE,*** macros, rendering of graphics and preloading mailed links at the e-mail clients.
2. ***USE E-MAIL SECURITY SOLUTIONS*** like anti-spam filters, malware scanners and URL analyzers to identify phishing websites in real-time.
3. ***KEEP YOUR MAIL CLIENT, OPERATING SYSTEM AND WEB BROWSER UPDATED AND PATCHED***. When the update notifications appear, install the updates as soon as they are available.
4. ***USE SECURE E-MAIL COMMUNICATION WITH DIGITAL SIGNATURES OR ENCRYPTION*** when exchanging sensitive information.
5. ***DO NOT CLICK ON LINKS OR DOWNLOAD ATTACHMENTS*** if you are not absolutely confident about the source of the e-mail.
6. ***USE TWO-FACTOR AUTHENTICATION*** to protect your accounts. If is implemented you should use, to prevent taking control of your account.
7. ***USE COMPLEX, STRONG AND UNIQUE PASSWORDS*** for every online service. Re-using the same password for various services is a serious security issue and should be avoided at all times.
8. ***DOUBLE-CHECK THE BANK RECIPIENT'S INFORMATION THROUGH A DIFFERENT CHANNEL***, when wiring money to an account.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

WEB-BASED ATTACKS

These types of attacks are methods by which cybercriminals can delude victims using web systems and services as threat vectors. This covers a vast attack surface, like creating malicious URLs to redirect the users to the other website, downloading malware or injecting malicious code into a website for stealing information.

Types of web-based attacks:

- **Drive-By Downloads** - downloads malicious contents to the victim's device. In this type of attack, the end-user visits a legitimate website compromised by cybercriminals with malicious scripts for running browser-based exploits or redirecting the user to another infected website.
- **Watering Hole Attacks** - targeted attacks using exploit kits with stealth features. A malicious actor is interested in compromising a specific group of users by using exploits or malicious content injected into the website.
- **Formjacking** - attackers inject malicious code into legitimate website's payment forms. This attack mostly captures banking and other Personal Identifiable Information (PII) and the malicious script will simultaneously forward the data to the portal and to the cybercriminals.
- **Malicious URL** - links created with the intention of distributing malware or facilitating a scam. The process involves socially engineering the victims' information to persuade them to click on the malicious URL, which delivers the malware and compromises the victims' computer.

HOW TO PROTECT

1. ***UPDATE THE SOFTWARE***

   Get the latest operating system, Internet browsers, application patches, plugins and add-ons and keep them updated and patched against known vulnerabilities.

2. ***ENDPOINT PROTECTION SOFTWARE***

   Use Heuristic File Protection Intrusion and Prevention System for a disk behavioral monitoring.

3. ***APPLICATION WHITELISTING***

   Isolate the applications and create a sandbox to reduce the risk of drive-by-compromise attacks.

4. ***USE A PROACTIVE APPROACH (SERVERS AND SERVICES)***

   Control the version of the content scripts as well as scanning locally hosted files and scripts.

5. ***RESTRICT THE WEB-BASED CONTENT***

   Use tools such as ad blockers for limiting the possibility of executing malicious codes while visiting specific websites.

6. ***MONITOR AND FILTER***

   Monitor and filter the web content and emails for detecting and preventing the delivery of harmful URLs and files.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

DoS AND DDoS ATTACKS

A Denial-of-Service (DoS) or a Distributed Denial-of-Service (DDoS) attacks represent malicious attempts to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Types of DoS and DDoS attacks:

- **Volume Based Attacks -** the attack's goal is to saturate the bandwidth of the attacked website. (UDP floods, ICMP floods, and other spoofed-packet floods).
- **Protocol Attacks -** this type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers. (SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more).
- **Application Layer Attacks** - comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server. (low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more).

HOW TO PROTECT

1

UNDERSTAND YOUR SERVICE

Understand the points where resources can be exhausted and who is responsible for them.

2

RESPONSE PLAN

Have a Denial of Service response plan in place that includes graceful degradation of your service.

3

REDUCE ATTACK SURFACE AREA

Minimize the surface area that can be attacked thereby limiting the options for attackers. Do not expose the resources to ports, protocols, or applications from where they do not expect any communication.

4

PREPARE THE SERVICE PROVIDERS

Ensure your service providers are prepared to deal with overloading of their resources and protect your service.

5

MONITOR AND TEST

Monitor for Denial of Service attacks and test your ability to respond.

6

UNDERSTAND THE WARNING SIGNS

Some symptoms of a DDoS attack include network slowdown, spotty connectivity on a company intranet, or intermittent website shutdowns. If a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDoS attack.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

WEB APPLICATION ATTACKS

The web application attacks range from targeted database manipulation to large-scale network disruption. These attacks can exfiltrate critical or personal information and make reputational damage.

Types of web-application attacks:

- **Cross-site scripting (XSS) -** upload a piece of malicious script code into the website for stealing data or perform other kinds of mischief.
- **SQL Injection (SQLi) -** submit destructive code into an input form. If the systems fail to clean this information, it can be submitted into the database where it can change, delete, or reveal data to the attacker.
- **Path traversal -** improper protection of data that has been inserted, these web server attacks involve injecting patterns into the webserver hierarchy that is allowed to obtain user credentials, databases, configuration files and other information stored on hard drives.
- **Local File Inclusion -** attack technique that involves forcing the web application to execute a file located elsewhere on the system.

HOW TO PROTECT

1. ***USE INPUT VALIDATION AND ISOLATION TECHNIQUES*** for injection type attacks.
2. ***USE AUTHORIZATION LEVELS AND STRICT AUTHENTICATION MECHANISMS*** to prevent breaches.
3. ***DEPLOY TRAFFIC AND BANDWIDTH MANAGEMENT CAPABILITIES*** and restrict access to inbound traffic for required services only.
4. ***SECURE DEVELOPMENT*** by applying security procedures in the application development and maintenance life cycle.
5. ***SCAN THE APPLICATION*** to discover any vulnerabilities and patch them as quickly as possible.
6. ***ENFORCE A GOOD PATCH MANAGEMENT AND TESTING PROCESSES*** for the web applications.
7. ***PERFORM VULNERABILITY AND RISK ASSESSMENTS*** before and during the process of web application development.
8. ***IMPLEMENT AN INVENTORY*** of the APIs used and validate them against perimeter scans discovery and encrypt the APIs' connection and communication.
9. ***INSTALL WEB APPLICATION FIREWALLS*** to control the access to web applications using rules designed to recognize and restrict suspicious activity.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

SOCIAL MEDIA SCAMS

Social media scams represent a criminal activity designed to trick someone through the use of social media platforms out of money or personal details, such as email addresses, passwords and birth dates.

HOW TO PROTECT

1 *PROTECT YOUR INFORMATION*

Avoid sharing details on social media that could enable someone to impersonate you and consider setting your profile to private.

2 *VERIFY REQUEST*

Verify any request that comes in from friends or acquaintances before you act upon it. Contact that person directly to ensure you are not being scammed.

3 *SECURE YOUR ACCOUNTS*

Create strong and unique password for all your online accounts. Don't use any type of personal details in your password.

4 *TAKE CARE ON PUBLIC WI-FI*

Avoid using apps with sensitive information while using public WI-FI connections.

5 *TREAT LINKS WITH SUSPICION*

Make sure you look closely at the URL before you log in to any social networking site. Be wary of shortened links.

6 *REFRAIN FROM TAKING A QUIZ*

Refrain yourself from taking social media catchy quizzes. Even if the quiz is legitimate, personal information is still being gathered.

7 *AVOID FREE APP DOWNLOADS*

Verify the source of the apps that ask for your social media personal information. Avoid third party app stores.

8 *BE AWARE OF CLICKBAIT*

Be aware of post that attract attention, whether claiming that gives out gift cards, wins in a lottery or some breaking celebrity news or photos.

9 *AVOID OVERSHARING*

Most people overshare. If in doubt, do not post. Oversharing can give criminals the information they need to social engineer you into falling prey to other scams.

10 *NEVER DOWNLOAD AN UNEXPECTED DOCUMENT ATTACHMENT*

Don't download an unexpected legitimate-looking document attached to a message that can download malware to your device and can steal personal information.

11 *GUARD AGAINST FAKE LIVE STREAM AND MOVIE OFFERS*

Avoid clicking on fake live streams or movies, that often go to websites that distribute malware, or request a credit card for a free trial.

SECURITY OF ONLINE TRANSACTIONS

Online transactions present a certain risk level regarding the undermining of personal data, but there are some methods that can limit this risk, using proper prevention means.

Types of attacks:

- **E-Skimming attacks** target traders who accept online payments, by changing the source code of online shops, managing this way to obtain in real time the access to clients' credentials.
- **Card-Not-Present (CNP) fraud** is a scam where the attackers attempt to make fraudulent transactions while not possessing the physical card.

HOW TO PROTECT

1. ***CHECK ONLINE SHOPS AND SELLERS*** to ensure that they are legitimate. A new e-commerce website can be a sign related to a possible fraud attempt.

2. ***CHECK FOR THE TRADER'S WEBSITE TO BE SECURED*** – use websites that benefit of both a digital certificate and a connection of https type (on the left of URL address you should be able to see a small locker).

3. ***AVOID INTRODUCING THE DATA FROM YOUR CREDIT-CARD ON THE WEBSITE.*** There are numerous websites where there are required the data of the credit-card for authentication, and once those credentials obtained they can be used later for unauthorized transactions.

4. ***GET INFORMED RELATED TO YOUR RIGHTS*** when you choose to purchase online goods and services and check the refund procedure.

5. ***TRY TO MAKE ONLINE PAYMENTS USING VIRTUAL CARDS*** that you can recharge only with the minimum amounts of money that you need for the transactions and that can be easily replaced in case they were compromised or try to use alternative systems of e-money, such as Paypal.

6. ***SOME SHOPS OF ONLINE TRADING OFFER TO THEIR CLIENTS THE POSSIBILITY TO STORE ONLINE THE DATA*** of their credit cards in order to facilitate the transactions. Carefully examine those situations and the risks that those websites of sellers to be compromised and this way to get access the access to your data.

7. ***NOTIFY AS SOON AS POSSIBLE THE COMPETENT AUTHORITIES,*** if you consider you have been the victim of a fraud,

8. ***BE VIGILANT!*** If an offer is too good to be true, maybe it is a false one!

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

SECURITY OF DEBIT / CREDIT CARD

Following some phone calls or some phishing campaigns via e-mail, the cyber criminals can ask you, under different reasons, the data of your credit card. The issuing financial institution or law authorities will never ask for these authentication data, therefore, if you already provided this data to another person, you have to immediately contact the bank in order to block the card.

HOW TO PROTECT

1. ***TAKE CARE OF YOUR CREDIT CARD*** as you take of your cash.

2. ***BE CAREFUL OF THE PIN CODE AND DO NOT KEEP IT INSCRIBED IN YOUR WALLET NEXT TO YOUR BANK CARD*** Avoid being seen by others when entering your PIN at the ATM / POS. Do not give your card PIN to another person.

3. ***WHEN YOU HAVE SUSPICIONS,*** check the official website of the bank or call the card issuing institution.

4. ***AVOID SENDING THE CARD'S AUTHENTICATION DATA*** by e-mail or other means of communication.

5. ***DO NOT REPLY TO INCOMING SMS MESSAGES ASKING FOR YOUR PIN CODE,*** data written on the card or other authentication elements such as online banking data.

6. ***KEEP THE CARD IN YOUR POSSESSION,*** don't share it and avoid leaving it in the car, on the restaurant table or in other public places.

7. ***SET MAXIMUM LIMITS ON ATM PURCHASES OR WITHDRAWALS*** to suit your needs and change these limits when necessary.

8. ***AVOID USING THE ATM IF YOU HAVE ANY SUSPICIONS*** - check the ATM in advance before making withdrawals or transactions.

9. ***DON'T FORGET TO PICK UP THE CARD*** after collecting the money from the ATM.

10. ***EMERGENCY TELEPHONE NUMBER.*** It is recommended that you have the bank's telephone number handy so that you can call and request a card lock when there are indications that the card data has been compromised or that you have lost your card or stolen it.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

IDENTITY THEFT

Identity theft or identify fraud is the illicit use of a victim's Personal Identifiable Information (PII) by an impostor to impersonate that person and gain a financial advantage and other benefits.

Types of techniques:

- **SIM-Swapping identities** - this technique targets cryptocurrency holders and high-profile individuals or accounts with the intention of stealing the victim's identity.
- **Digital doppelgangers** - the anti-fraud technique 'digital masks' was exposed when stolen digital identities appeared as a trading product on the darknet marketplaces.
- **Business e-mail compromise (BEC)** - the attackers impersonate a trusted individual, usually within the company, and the victim is tricked into making a financial transaction or divulging sensitive information, personal or corporate.

HOW TO PROTECT

1. ***AVOID USING THE PASSWORD MANAGER PROVIDED BY THE BROWSER.*** If one is needed, use an offline protected password manager.
2. ***MULTI-FACTOR AUTHENTICATION IS A SECURITY MEASURE*** to overcome password hacking or loss and to ensure the success of the authentication process with multiple keys.
3. ***AUTHENTICATE ANY SENDER OF A REQUEST*** to transfer money by telephone or in person.
4. ***ADEQUATELY PROTECT ALL IDENTITY DOCUMENTS AND COPIES*** (physical or digital) against unauthorized access.
5. ***DO NOT DISCLOSE IDENTITY INFORMATION*** to unsolicited recipients and requests by phone or e-mail or in person should not be answered.
6. ***ENFORCE THE USE OF PASSWORD PROTECTED DEVICES,*** ensuring good quality of credentials, and secure methods for their storage.
7. ***PAY CLOSE ATTENTION WHEN USING PUBLIC WI-FI NETWORKS.*** If one is used, avoid accessing sensitive applications and data. Use a trusted VPN service to connect to public Wi-Fi networks.
8. ***ENSURE GOOD QUALITY OF CREDENTIALS AND SECURE METHODS*** for their storage in all used media.
9. ***CHECK TRANSACTIONS DOCUMENTED*** by Bank Statements or received receipts regularly for irregularities.
10. ***INSTALL CONTENT FILTERING*** to filter out unwanted attachments, mails with malicious content, spam, and unwanted network traffic.

INSIDER THREATS

An insider threat is a malicious threat to an organization that may result in an incident, performed by someone or a group of people affiliated with or working for the organization.

HOW TO PROTECT

1 *ESTABLISH PROGRAM*

Deploy a deep packet inspection (DPI) technology for anomaly detection. Adopt a user-focused view in order for security teams to spot insider threat activity.

2 *TRAIN YOUR TEAM*

An engaged workforce trained to recognize and report suspicious behavior or activity can help defend against insider threats.

3 *REDUCE ACCESS*

Reduce the number of users with privileges and access to sensitive information.

4 *ASSIGN RISK SCORES*

Cognitive applications for behavioral analytics can assign risk scores to proactively identify potential insider risks before a breach has occurred.

5 *INTRODUCE COUNTERMEASURES PLAN*

Include a risk management framework, business continuity plan, disaster recovery program, a financial and accounting management policies, and a legal and regulatory management.

6 *IMPLEMENT ROBUST TECHNICAL CONTROLS*

Implement data loss prevention (DLP) to protect assets and to prevent data exfiltration.

7 *HARDEN THE DIGITAL ENVIRONMENT*

Be aware of the security of the network, systems, applications, data, and accounts.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

DATA PROTECTION REQUEST FROM INDIVIDUALS

There are specific requirements for filing, responding to and permitting full exercise of individual's rights under the GDPR.

MAIN PRACTICAL POINTS

1

SUBMITTING REQUESTS

Use the channels set up by the organization. Be specific about the situation/data/type of request. Provide sufficient details and documents.

2

RESPONDING - PROCEDURE

Check:
(a) how authentication steps can be set,
(b) requirement to notify organizations to whom you disclosed data,
(c) conditions for extensions to response deadline. Disclose responses in a secure manner.

3

RESPONDING – CONTENT

Check:
(a) both structured and unstructured data,
(b) data held by data processors,
(c) if confidential data/trade secrets can/ should not be disclosed.

4

DATA ACCESS

Request specificity if too general and entails significant amount of data. Check any conflicting legal requirements – e.g. confidentiality legal obligations.

5

RECTIFICATION OF DATA

Replicate changes in all IT systems, with data processors and all locations where data is held. Check accuracy of data provided.

6

PORTABILITY

Prepare data in a structured, commonly used and machine-readable format (e.g. .csv). Send data to individual/to the organization indicated by him/her.

7

AUTOMATED DECISIONS

Provide sufficient details for individuals to understand the decision algorithm and process. Check mechanism of automated decision and consequence/impact on individual.

8

OBJECTION, ERASURE AND RESTRICTION OF PROCESSING

Check if reasons to reject request are applicable. Apply measure to all replications of the personal data in the organization and with data processors.

DATA PROTECTION COMPLIANCE FOR SMEs

The four areas to be considered are:
(1) Data flows (inside and to/from outside the organization)
(2) IT systems involved in the data flow
(3) Disclosure of data to/from other organizations
(4) Appropriate internal procedures.

MAIN STEPS TO BE TAKEN

1 *DATA FLOW AND PURPOSE*

Identify
(a) collection, storing, processing and disclosure of data
(b) processing basis
(c) location of data
(d) initial and subsequent processing purposes.

2 *DATA MINIMISATION*

Collect, store, process, disclose only the types/amount of data needed.

3 *TRANSPARENCY OF PROCESSING*

Adequately inform individuals about the processing of their personal data generally prior to collection/processing.

4 *TAILORED SECURITY MEASURES*

(a) access limitation based on need-to-know principle
(b) protect data in transit and data at rest
(c) confidentiality, integrity, and availability controls based on data held by and role of the IT system in the data flow.

5 *THIRD PARTY MANAGEMENT*

(a) identify personal data disclosure
(b) conclude appropriate agreements
(c) monitor/ensure proper compliance continuously.

6 *PRIVACY ASSESSMENT*

Perform specific analysis to ensure appropriate protection of the rights of individuals by reference to the interest/scope of the organization.

7 *INTERNAL PROCEDURES AND PROCESSES*

(a) Plan (all of the above, including incident handling, responding to requests from individuals)
(b) Do (appropriate implementation tools)
(c) Check (continuous monitoring of implementation)
(d) Act (lessons learnt from auditing, monitoring, investigations, data breaches)
REPEAT.

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

TRANSPARENCY OF PERSONAL DATA PROCESSING

Information notice provided to individuals whose personal data is processed reflecting the data processing specifics, including prior to obtaining consent (if this is the processing basis).

MAIN ASPECTS TO CONSIDER

1 *FORM OF THE INFORMATION NOTICE*

Structured text or visual methods (e.g. infographics). Entire information notice at once or layered approach.

2 *BRINGING TO THE ATTENTION OF INDIVIDUALS*

Generally, at the outset of data collection/establishing new processing purpose. Easily accessible (e.g. pop-up) at the outset and for future consultation.

3 *PROCEDURAL STEPS*

Make sure individuals read it (e.g. tick box for acknowledgement of reading). Keep proof of this action (e.g. logs). Keep versioning history.

4 *CONTENT OF INFORMATION NOTICE*

Concise, clear (no interpretable phrases), intelligible, easy to understand based on specifics of individual (e.g. child).

5 *MAIN DETAILS TO BE INCLUDED*

Scope and basis for processing. Disclosure to other organizations. Storing period before deletion. Types of personal data processed. Transfers outside the EU. Details on automated decisions.

6 *CONSENT MANAGEMENT*

Allow easy withdrawal of consent. No pre-checked boxes for obtaining consent. Retake consents after a period of time.

7 *CONTENT OF CONSENT*

Granularity, for each processing purpose. Specifically detailed for the processing purpose. Proper information notice before obtaining consent.

8 *CONDITIONS FOR TAKING CONSENT*

Clear action of the individual. Freely given (no conditioning, subordination, or negative consequences if consent not given).

CYBERSECURITY GUIDE, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.EN

NIS DIRECTIVE

NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The Directive is transposed in Romania by the Law no. 362/2018 on ensuring a high common level of security of networks and information systems.

MAIN ELEMENTS OF THE DIRECTIVE

1. ***ENSURES THAT THE OPERATORS OF ESSENTIAL SERVICES (OES) FROM A SET OF KEY-SECTORS*** take appropriate security measures and notify significant incidents to national authorities.

2. ***ADDRESSES OES, WHICH ARE PRIVATE BUSINESSES OR PUBLIC ENTITIES WITH AN IMPORTANT ROLE TO PROVIDE SECURITY IN THE FOLLOWING SECTORS:*** healthcare, transport, energy, banking, and financial market infrastructure, digital infrastructure, and water supply.

3. ***HARMONIZATION AT THE EU LEVEL,*** especially on OES identification and security measures, is needed for reaching a similar level of cyber-resilience of the internal market and because cyber-threats have a cross-border impact.

4. ***THE DIRECTIVE ENSURES SMOOTH FUNCTIONING OF THE INTERNAL MARKET*** through adopting security measures that help reach a high common level of security of network and information systems across the Union.

5. ***THE NATIONAL INSTITUTIONAL FRAMEWORK*** is updated by designating a national authority with regulatory, supervisory, and control responsibilities, a Single Point of Contact the national level, and the national CSIRT team.

6. ***CREATES A COOPERATION GROUP*** composed of representatives of the Member States, the Commission, and ENISA. The role of the Group is to support and facilitate strategic cooperation and the exchange of information. It also fosters trust and confidence among the Member States.

7. ***CREATES A CSIRT NETWORK*** composed of national CSIRTs and CERT-EU. Its most important role is to exchange information, coordinate responses to incidents, and offer support in addressing cross-border incidents.

8. ***ENCOURAGES THE ADOPTION OF A NATIONAL STRATEGY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS*** defining strategic objectives and priorities, governance to achieve them, measures, education and awareness, R&D.

INCIDENT REPORTING

Emergency call: 1911

How to report?

By calling to the single emergency number **1911** or by writing an e-mail at **alerts[@]cert.ro**.

Who should report?

Individuals and legal entities can call this unique number if they are victims of a cyber-incident.

What types of incidents?

Vulnerable computer systems are compromised or infected with various types of malware. Malicious activities, such as but not limited to scams, phishing, fraud, and vishing.

How can we help?

Firstly, we offer support, assistance, and sorting (ticketing). The technical support helps the potential victim to reduce or eliminate the threat. The second step is analyzing the information to support the incident response and create a cybersecurity alert. If the reported incident is subject to a criminal offence, we direct the potential victim to the law enforcement authorities (e.g. Police).

NIS Directive

How to report?

Firstly, by formal reporting, containing specific information, through a dedicated platform. Following is the information sharing and collaboration on the Malware Information Sharing Platform (MISP).

Who should report?

Operators of essential services are mandated to immediately notify CERT-RO, acting as national CSIRT, of incidents that have a significant impact on the continuity of the essential services they provide.

What types of incidents?

Notify the incidents that exceed the significant impact thresholds on the delivery of the essential service. The criteria to establish the impact are the number of affected users, duration, geographical distribution of the attack.

How can we help?

After the notification, we evaluate the impact of the incident and create an alert. The national CSIRT team coordinates the incident response and offers the affected entity information to support incident management.

CVD*

How to report?

By writing an e-mail at **cvd[@]cert.ro**, containing all the technical details, including a description of the vulnerability, steps, and the techniques to replicate it, and the means of discovery.

Who should report?

Professionals and non-professionals of computer networks and systems that have identified a vulnerability as users of a service or computer system offered to the public and want to report it for remediation.

What types of incidents?

Any type of vulnerability of a service or computer system offered to the public.

The role of CERT-RO?

Assures the framework for CVD activity, issues guidelines, and useful information, and offers public recognition when the stakeholders wish it.

Coordinated Vulnerability Disclosure

REFERENCES

1. Cybersecurity and Infrastructure Security Agency (CISA), Publications on cybersecurity. Available: https://us-cert.cisa.gov/security-publications.
2. European Union Agency for Cybersecurity (ENISA), Publications from the Threat Landscape 2020 Series. Available: https://www.enisa.europa.eu/publications.
3. European Union Agency for Law Enforcement Cooperation (EUROPOL), Publications and documents on cybercrime. Available: https://www.europol.europa.eu/publications-documents.
4. European Union Agency for Law Enforcement Training (CEPOL), E-Journals on cybercrime. Available: https://www.cepol.europa.eu/science-research/journals/e-journals.
5. European Institute of Romania, Current challenges in the field of cybersecurity – the impact and Romania's contribution to the field. Available: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf.
6. International Journal of Information Security and Cybercrime (IJISC). Available: https://www.ijisc.com/.
7. Romanian Association for Information Security Assurance (RAISA), Considerations on challenges and future directions in cybersecurity. Available: https://www.raisa.org/documents/CybersecurityRO2019.pdf.
8. Romanian National Computer Security Incident Response Team (CERT-RO), Cybersecurity guides. Available: https://cert.ro/doc/ghid.
9. National Association for Information Systems Security (ANSSI), Guide for securing computers and networks. Available: https://cert.ro/vezi/document/ghid-bune-practici-pentru-securizarea-calculatoarelor-personale.
10. National Cyberint Center within the Romanian Intelligence Service, Best practices guide for cybersecurity. Available: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf.

ACRONYMS

API - Application Programming Interfaces
APT - Advanced Persistent Threat
ATM - Automated Teller Machine
CD / DVD - Compact Disc / Digital Versatile Disc
CERT- Computer Emergency Response Team
CMS - Content Management System
CSIRT - Computer Security Incident Response Team
CVD - Coordinated Vulnerability Disclosure
DDoS - Distributed Denial of Service
DLP - Data Loss Prevention
DoS - Denial of Service
DPI - Deep Packet Inspection
GPS - Global Positioning System
ICMP - Internet Control Message Protocol
IDPS - Intrusion Detection and Prevention Systems
IoT - Internet of Things
IP - Internet Protocol
LAN - Local Area Network
MAC (address) - Media Access Control
OES - Operators of Essential Services
OS - Operating System
PDF - Portable Document Format
PII - Personal Identifiable Information
PIN - Personal Identification Number
POS - Point of Sale
QR (code) - Quick Response
SIEM - Security Incident and Event Management
SME - Small and Medium-sized Enterprises
SOHO - Small Office / Home Office
SQL - Structured Query Language
SQLI - SQL Injection
SSID - Service Set Identification
UDP - User Datagram Protocol
URL - Uniform Resource Locator
USB - Universal Serial Bus
VPN - Virtual Private Network
WPA2 (protocol) - Wi-Fi Protected Access
XSS - Cross-Site Scripting

AUTHORS

Iulian ALECU is the Deputy General Director of the Romanian National Computer Security Incident Response Team (CERT-RO), with an experience of more than eight years in cybersecurity and related international cooperation. He was the Chair of the Cooperation Group during the Romanian Presidency at the Council of the European Union.

Costel CIUCHI, PhD, is a Senior Expert in the Information Technology and Digitalization Directorate, General Secretariat of the Government with responsibilities in developing government apps and infrastructure, security of IT services (INFOSEC) and coordinating Gov.ro Domain Registry. Associate Professor at University Politehnica of Bucharest, he conducts research activities in decision making, cybersecurity and security risk area.

Toma CÎMPEANU, has more than 20 years' experience in the ICT field, holding top positions in both public and private companies and contributing to several nationwide projects such as e-licitatie.ro, ghiseul.ro, Romanian National Point of Single Contact (PCUe), Ro-Net and other. Since 2015, he is the CEO of the National Association for Information Systems Security (ANSSI).

Iulian COMAN is a Seconded National Expert at the European Union Agency for Law Enforcement Training (CEPOL), police officer in the Ministry of Internal Affairs, Romania, with expertise in analysis, law enforcement training and international relations. He is a PhD candidate in public order and national security domain with the 'Alexandru Ioan Cuza' Police Academy Bucharest.

Larisa GĂBUDEANU is a data protection expert and a PhD candidate at the Babeş-Bolyai University. With a vast experience as a lawyer in an international law firm, counselling international clients and coordinating projects related to IT law and data protection matters, she also has good knowledge of information security gathered in a regional banking group and from her academic background in information security.

Ioan-Cosmin MIHAI, PhD, is a researcher, professor, trainer, and conference speaker, with an experience of more than 15 years in cybercrime and cybersecurity. He is associate professor at "Al. I. Cuza" Police Academy, visiting professor at the University Politehnica of Bucharest and "Carol I" National Defence University, Romania, and vice president of the Romanian Association for Information Security Assurance (RAISA).

Cosmina MOGHIOR is a Public Policy Expert at CERT-RO, where she represents the institution in the NIS Cooperation Group and provides expertise in the European Cybersecurity Certification Group. She is also an active academic, being a Ph.D. Candidate at the National School of Political and Administrative Studies, with the thesis "European Digital Sovereignty: Technological Independence in the Context of Strategic Confrontation."

Nelu MUNTEANU is the Technical Director of the Romanian National Computer Security Incident Response Team (CERT-RO), with an experience of more than 18 years in IT&C and cybersecurity domains. He has been managing the technical department at CERT-RO since 2016 and participating on many activities dedicated to increase the awareness level and education on cybersecurity.

Gabriel PETRICĂ, PhD, has an extensive experience acquired in over 25 years of work in ICT field. With a PhD in Electronics, his area of interest includes the dependability of systems, Web programming and information security. Currently he performs teaching and research activities within the Faculty of Electronics, Telecommunications and Information Technology from the University Politehnica of Bucharest.

Ionuţ STOICA is Senior Project Officer within the Council of Europe, Cybercrime Programme Office, with an experience of more than 14 years' experience in cybercrime investigations and trainings. He is currently involved in capacity building programs on cybercrime and he is also a trainer on cybercrime for the Romanian Banking Institute.

Cătălin ZETU is leading the Cyber Attacks Office, part of the Romanian Central Cybercrime Unit, with wide responsibilities from investigations, to intelligence and strategy. Cătălin is developing strong partnership with private partners in order to bust the overall capacity of the unit. He is a very experienced cybercrime investigator that worked or supervised high profile cases with multiple international ramifications.

Romanian Association for Information Security Assurance

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit and public benefit association. Founded in 2012, RAISA started as an initiative dedicated to promote the information security.

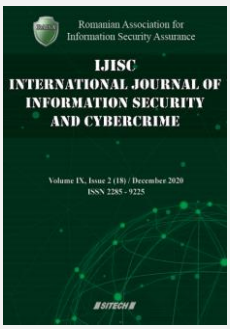
The aim of the Romanian Association for Information Security Assurance (RAISA) is promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment from Romania.

The vision of the Association is to promote research and education in information security field and to contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at the national level, bringing together professors and researchers from top universities and Romanian institutions, PhDs, Master's students and undergraduates, as well as companies from the IT segment.

Website**:** www.raisa.org (EN) / www.arasec.ro (RO)

RAISA supports scientific work in the fields of cybersecurity and cybercrime by publishing and promoting books, technical studies, and the publication of *International Journal of Information Security and Cybercrime (IJISC)*, a biannual scientific journal with the purpose of analyzing information, computers systems and communications security and identifying new valences of cybercrime phenomenon.

Website: www.ijisc.com



RAISA portals and media channels:

INFO SECURITY WEB PORTAL
www.securitatea-informatiilor.ro

CYBER SECURITY WEB PORTAL
www.securitatea-cibernetica.ro

NET SECURITY WEB PORTAL
www.securitatea-retelelor.ro

CYBER CRIME WEB PORTAL
www.criminalitatea-informatica.ro

CYBERSECURITY GUIDE