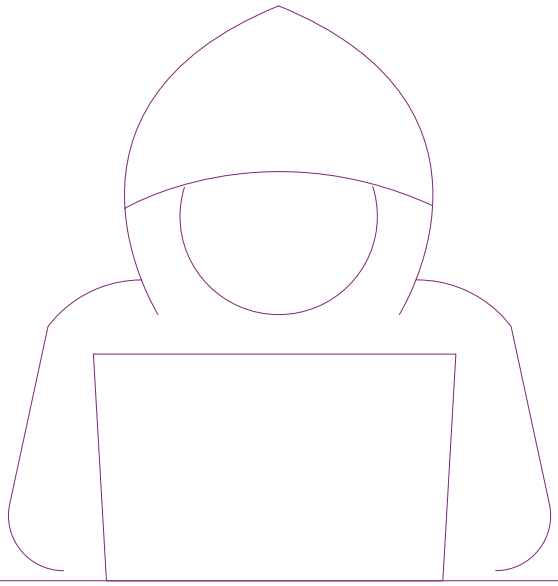
UK Government

INSTITUTE FOR WAR & PEACE REPORTING

IWPR

Cyber resilience for women's rights organisations

A GUIDE FOR ACTIVISTS, PEACEBUILDERS, AND ADVOCATES



Written by: **Jennifer Kanaan**
Edited by: **Daniella Peled**
Designed by: **Humblebee-Design**

Cyber resilience for women's rights organisations

A GUIDE FOR ACTIVISTS, PEACEBUILDERS, AND ADVOCATES

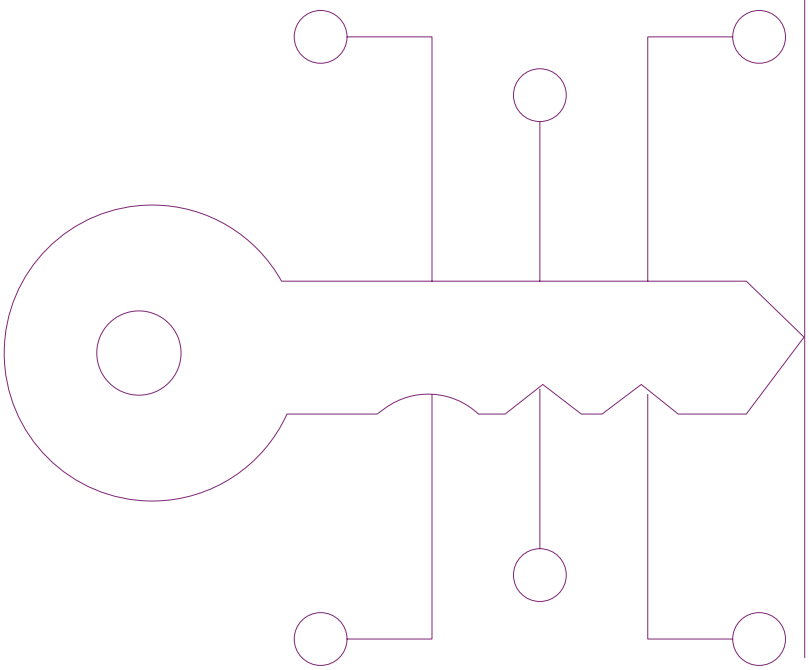
This publication was prepared under the "Building Resilience in the Eastern Neighbourhood" project (BREN), implemented with the support of the United Kingdom's Foreign Commonwealth and Development Office (FCDO). The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the UK Government.

Delivered in partnership with the Global Network of Women Peacebuilders (GNWP), BREN is designed to strengthen the resilience of civil society organisations and promote human security, peace and stability in South Caucasus and Moldova, particularly for women and other marginalised communities.

The Institute for War & Peace Reporting (IWPR) empowers local voices to drive change in countries of conflict, crisis and transition. Where hate speech and propaganda proliferate, and journalists and civic activists are under attack, IWPR promotes reliable information and public debate that makes a difference.

The information provided in this guide does not, and is not intended to constitute cybersecurity advice; instead, it is intended for general informational purposes only.

It is crucial for organisations to engage a cybersecurity advisor, consultant, or, at the very least, an IT expert to support the organisation in fortifying its cyber environment. These experts can provide assistance, guidance, and swift responses in the event of an attack or other issues.



INSTITUTE FOR WAR & PEACE REPORTING

IWPR

Bio Jennifer Kanaan:
Jennifer Kanaan is the regional communication manager for the Building Resilience in the Eastern Neighborhood programme (BREN) at the Institute for War & Peace Reporting (IWPR). A digital communication and advocacy expert, Jennifer has been with IWPR since 2016, contributing to diverse projects. These include the pioneering "Cyber Arabs" project, IWPR's comprehensive Arabic-language cybersecurity resource website and a digital advocacy manual for Etihad, a project supporting LGBTQI organisations in the MENA region.

Bio Daniella Peled:
Daniella Peled is the managing editor of IWPR, overseeing all editorial content and production. A journalist and editor with more than 20 years experience of reporting foreign affairs, she has also designed and implemented journalism training in many of IWPR's areas of operation including Afghanistan, Iraq and Turkey.

Thanks to:
Cyber Experts: Samvel Martirosyan, Artur Papyan, Davit Ghonghadze, and Vlad Mazureac

gnwp Global Network of Women Peacebuilders

Gender analysis in cyber threats

Cyber threats have emerged as a pervasive issue impacting individuals worldwide. Unfortunately, women often bear the brunt of these threats, facing unique challenges and vulnerabilities. Across the globe, cyber violence against women is a pressing concern, encompassing forms such as cyberharassment, revenge porn and online attacks with violent undertones (1, 2, 3) These attacks often escalate into serious threats, exemplified by incidents targeting female journalists with death threats in Bosnia Herzegovina (4).

A 2023 study on Gender and Human Rights in National-level Approaches to Cybersecurity by GNWP emphasises the importance of incorporating a gender perspective into policy-making. This approach recognises that women and women's rights organisations may face unique challenges that need tailored analyses and recommendations.

According to the GNWP report, the benefits of applying a gender lens to cybersecurity include:

1 Acknowledging that women and marginalised groups use the internet differently and are disproportionately harmed by cyber attacks. Their specific needs and representation in cybersecurity policymaking and technology development are often overlooked.

2- Improving access to cybersecurity provisions for women and other marginalised groups, addressing limitations in emergency response and legal remedies due to pre-existing discriminatory societal structures.

3- Addressing blind spots in cybersecurity policy by incorporating a gendered perspective, emphasising a human-centric and gender-sensitive approach.

Am I really a target?

Absolutely, you are. In fact, everyone is.

The intention here is not to instil panic or fear. However, it is crucial to be pragmatic and gain a clear understanding of cyber threats and criminal activities. This knowledge will empower you to navigate these challenges and safeguard not only yourself but also your colleagues, beneficiaries and your work.

Whether you are a humanitarian, activist, or women's rights defender, your focus is likely to be advocating for change, lobbying for gender perspectives in legislation and raising awareness in your communities.

Cyber threats might not be part of your usual considerations, and you certainly cannot be expected to approach situations like a cyber criminal. Yet, similar to incorporating a gender lens into policies and laws, it's imperative in today's world to integrate cyber awareness into all your activities.

> By safeguarding yourself, your colleagues, and your organisation, you are not just protecting data; you are securing the positive impact you have and will continue to make on society

Let's meet Leyla and Malika

Leyla, a passionate women's rights advocate, dedicates her days to instigating positive change. Her routine includes meetings with local women's organisations, strategising to advance gender equality and mentoring young activists. She spends many evenings in community outreach programmes, where she shares empowering stories to inspire women. Leyla's day is a blend of advocacy, education and uplifting conversations.

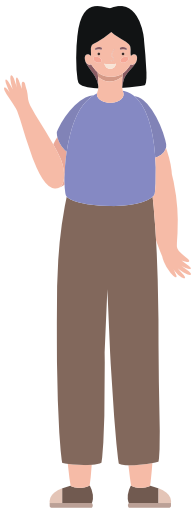
Malika, a committed peacebuilder and community leader, focusses on grassroots initiatives. Actively engaged in fostering dialogue and understanding, Malika often leads community workshops and organises peacebuilding events, promoting unity among diverse groups. Her commitment also extends to evening discussions on conflict resolution, engaging with community members. Her typical day is filled with by meetings, workshops and collaborative efforts to build a peaceful and inclusive society.

Leyla

WOMEN'S RIGHTS ADVOCATE

Job History: Leyla is a prominent women's rights activist, dedicating her career to advancing gender equality and justice. Her work focuses on empowering women in post-conflict regions, contributing to sustainable peace.

Lifestyle: Leyla is deeply involved in community-building initiatives and peace dialogues. Her commitment to inclusivity and social justice has made her a respected figure among women's rights advocates.

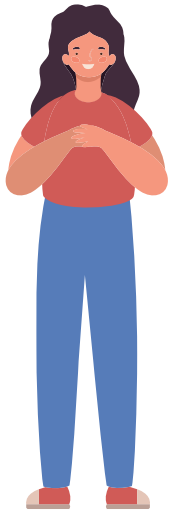


Malika

PEACEBUILDER AND COMMUNITY LEADER

Job History: Malika is a dedicated peacebuilder actively involved in initiatives addressing war, violence, and social inequalities. She co-founded her own peacebuilding initiative, fostering dialogue and understanding.

Lifestyle: Malika leads community workshops, emphasizing the importance of women's involvement in peace processes. Her focus on grassroots efforts exemplifies the intersection between peacebuilding and women's rights.



Why target activists, peacebuilders, and community leaders?

Cybercriminals target individuals in these roles due to their influential positions in society. Their efforts towards positive change make them potential threats to those with opposing interests. Additionally, the nature of their work often involves sensitive information, making them attractive targets.

TYPES OF CYBER ATTACKS SIMPLIFIED:

Untargeted attack:
- The most common form of malicious threat.
- Does not pinpoint specific individuals or organisations.
- Cyber criminals aim to target as many computers, individuals, and organisations as possible.
- Malware, worms or viruses are sent indiscriminately via email to numerous addresses.
- Untargeted cyberattacks are easier to execute but are less destructive than targeted attacks.

Targeted attack:
- Aimed at a particular person or organisation.
- Cyber criminals operate with a specific aim, singling out a target of interest.
- These attacks take months to execute and can involve social engineering, phishing, tailor-made malware, persistent campaigns and botnets.
- Targets have expanded beyond government bodies and military bases to include organisations, media, communications and critical infrastructure

Understanding these concepts will empower you to navigate the digital landscape effectively.

You're likely wondering, "Why would cyber criminals bother targeting me?" It's a valid question, especially for those dedicated to humanitarian, activist or women's rights causes. The motivations behind cyber attacks may seem perplexing, but understanding them is crucial.

MOTIVATIONS UNVEILED: WHY TARGET YOU?

1. Influence and Disruption:
Your vital role: As an activist, peacebuilder or community leader, your mission is to shape public opinion and influence policies..

The cyber threat: Cyber criminals may set their sights on you to disrupt your impactful work. By targeting you, they aim to create chaos, undermining the positive initiatives you champion.

2. Obtaining sensitive information:
Handling critical data: : In your daily endeavours, you often deal with sensitive information related to social issues.

The cyber threat: Cyber criminals might seek to steal or manipulate this data for their own gain. Whether it's for personal profit or to sway public opinion, your valuable information becomes a target.

Understanding these motivations is the first step to fortifying your cyber resilience.

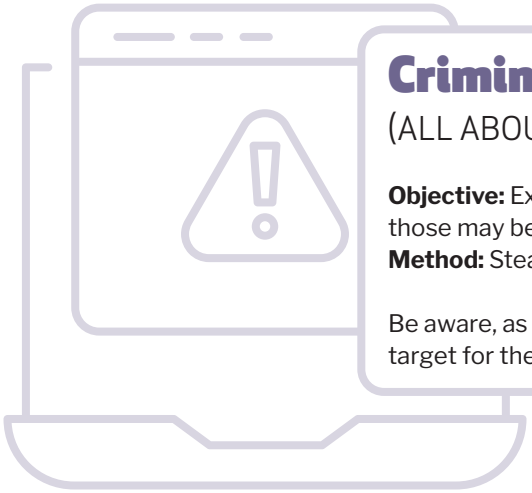
> Our role as Cyber Security experts is to protect you from being a random victim (untargeted attack). If a hacker actually targets you, they will most likely find a way or a vulnerability, our role here is to delay this as much as possible
>
> VLAD MAZUREAC, CYBER SECURITY EXPERT

Your quick guide to the types of cyber criminals

Hacktivists:
(YES, THEY REALLY EXIST!)

Motivation: Driven by political or social causes.
Mission: Advocate for their agenda or protest perceived injustices.
Favourite Cyber Attacks: Defacing websites, leaking sensitive information, or disrupting online activities.

The nature of your work could indeed make you a target for hacktivists. Stay informed and vigilant.



Criminal organisations:
(ALL ABOUT THE MONEY)

Objective: Expand their criminal activities (whatever those may be).
Method: Steal private data to sell for profit.

Be aware, as your valuable data could be a lucrative target for these organisations.

State-sponsored actors
(FOREIGN OR DOMESTIC)

Involvement: Governments or state-sponsored entities.
Objective: Suppress dissent and monitor opposition activities.
Risk Level: Advanced capabilities pose a high risk to individuals and organisations alike.

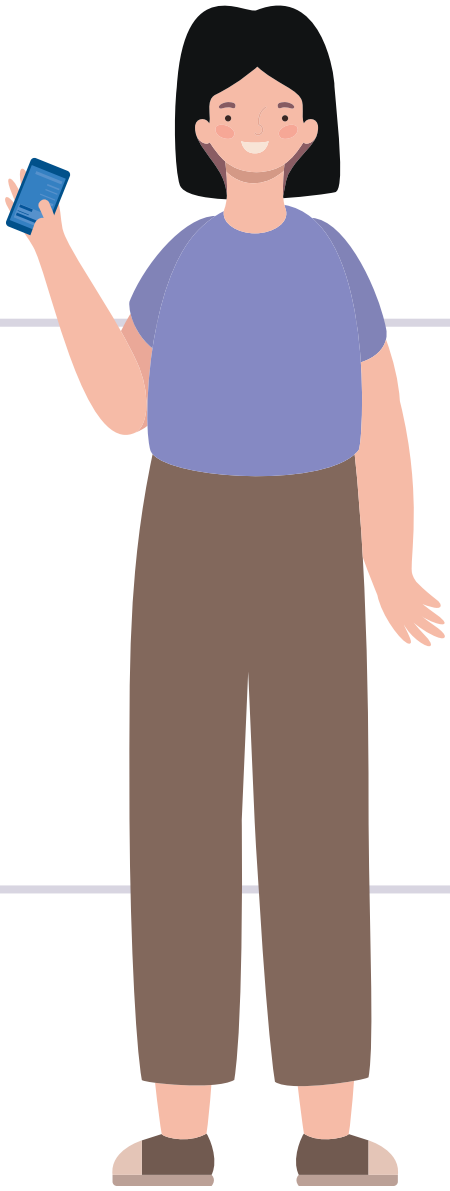
Understanding the motivations behind cyber threats against activists, peace builders, and community leaders is pivotal. It empowers you to recognize potential threats and take proactive steps to develop robust cybersecurity measures.

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

1. **Universal vulnerability:** Everyone is susceptible to cyber attacks. Your professional role might elevate this risk.
2. **Targeted vs. untargeted attacks:** The primary distinction lies in intent. Targeted attacks aim at specific individuals, while untargeted attacks cast a wider net.
3. **Diverse cyber criminal motivations:** Various types of cyber criminals exist, each driven by unique agendas and motivations.
4. **Holistic protection:** Prioritizing your cyber safety doesn't just shield you; it extends protection to your colleagues, beneficiaries, and organisation.

Remember, understanding these key aspects not only fortifies your individual defences but also contributes to the collective resilience of your professional ecosystem.

> Know your enemy and know yourself, and you can fight a hundred battles without disaster
>
> SUN TZU



TEST YOUR KNOWLEDGE

Leyla, a prominent activist, received a phishing email claiming to be from a human rights organisation with which she collaborates. The email urged her to click a link to update her credentials due to a security breach

What type of cyber attack was she a victim of?

1. Targeted attack to steal her data
2. Untargeted attack to steal her data
3. Targeted attack from a criminal organisation
4. Untargeted attack from a criminal organisation

The answers can be found in the last chapter: Cyber Answers

Safe internet browsing: Would you walk on a busy street with your bag open?

Certainly not!

Imagine strolling down a bustling street in the heart of the city on your way to work. Ensuring your bag is securely closed, glancing both ways before crossing the street, and staying attuned to your surroundings will have become second nature to you. Even in seemingly secure spaces, maintaining awareness, exercising caution and taking proactive measures to reduce risk become ingrained habits.

The same principles apply when navigating the online world. Safe internet browsing mirrors the principles of a secure stroll through the streets, emphasising awareness, caution and proactive steps to minimise risk.

Empower yourself to become more vigilant in the digital realm. Cybercriminals employ increasingly sophisticated techniques to deceive and steal data. While it may be challenging initially, adopting these practices is similar to the habits you employ when navigating the streets or leaving your apartment – they become second nature with practice.

Aspect	Safe strolling through the streets	Safe internet browsing
Vigilance and awareness	Stay aware of surroundings, avoid poorly lit areas, and be cautious of unfamiliar individuals.	Be cautious of phishing scams and fraudulent websites.
Verification of safety	Choose safe routes and verify the credibility of the neighbourhood for physical safety.	Verify the authenticity of websites before sharing personal information.
Preventive measures	Adopt preventive measures like locking doors, closing your bag and securing valuables.	Utilise security tools, update browsers, and employ strict privacy settings.
Adherence to rules and guidelines	Obey traffic rules, and follow street signs and guidelines.	Follow cybersecurity best practices and adhere to online rules.
Periodic checks for security	Conduct periodic checks of locks, doors, and surroundings for physical security.	Regularly update operating systems, browsers, and security software.

LEVON DARBANYAN | UNSPLASH

Your quick guide to spotting fraudulent websites

1 **Check the URL:** Scrutinise the website's URL for misspellings, extra characters, or unusual domains.
- **Legitimate:** https://www.example.com
- **Phishing:** https://www.exaample.com (misspelling), https://www.example.pf (unusual domain)

2 **Look for HTTPS:** Ensure the website uses HTTPS instead of HTTP. The 'S' indicates a secure connection with encryption for data transmission.
- **Legitimate:** https://www.securewebsite.com
- **Phishing:** http://www.insecurewebsite.com (lacks the 'S' for secure)

3 **Verify the Website Design:** Be cautious of poorly designed websites or those with numerous pop-ups.
- **Legitimate:** Professional layout, consistent branding.
- **Phishing:** Poor design, mismatched logos, numerous pop-ups.

4 **Check for Contact Information:** Legitimate websites provide clear contact information. Be suspicious if none is available or if the details seem dubious.
- **Legitimate:** Clear contact page with a valid address, phone number, and email.
- **Phishing:** No contact information or suspicious details like a generic email address.

5 **Hover over links:** Hover your mouse over links to preview the destination URL. Avoid clicking on links in emails; instead, type the URL directly.
- **Legitimate:** Hovering over a link shows a preview matching the displayed text.
- **Phishing:** Hovering reveals a different destination URL, e.g., http://www.trustworthy.com (displayed) but leads to http://www.phishingsite.com.

Fraudulent websites:

SIMPLY EXPLAINED

What are they? Fraudulent websites are illegitimate online platforms designed to deceive visitors into providing personal or financial information.
How? By creating sites that mimic trustworthy entities, aiming to trick users into disclosing sensitive data.
Where? Banks, e-commerce stores, dating sites, etc.

Your quick guide to spotting phishing scams

1 **Check your accounts regularly:** A phishing email may claim suspicious activities on your account, urging you to click a link to resolve the issue.
Example: "Urgent: Your account has been compromised. Click here to verify."

2 **Emails demanding urgent action:** Phishers create a sense of urgency.
Example: "Your account will be suspended unless you confirm your details within 24 hours. Click now to avoid disruption."
Example: "Act now to claim your reward before it expires!"

3 **Emails with bad grammar and unprofessional spelling:** Legitimate organisations maintain professional communication.
Example: "Dear user, your accoount has been compremised. Please update your password for securitee."
Example: "Click here for your exclusive pr1ze" instead of "Click here for your exclusive prize."

4 **Use of a public email domain:** Phishing emails may use generic email domains.
Example: "service@gmail.com" instead of "service@legitimatecompany.com."

5 **Check the email address:** Cybercriminals mimic legitimate email addresses.
Example: "support@paypa1.com" instead of "support@paypal.com."

6 **Generic subject line:** Phishing emails often have vague subjects.
Example: "Important Information" without specifying the nature of the message.

Phishing scams:

SIMPLY EXPLAINED

What is it? Phishing scams are fraudulent attempts to trick individuals into divulging sensitive information, such as usernames, passwords, or financial details, which can then be used for malicious purposes.
How? By posing as trustworthy entities in emails, messages, or other forms of communication.
Where? Emails, social media, Whatsapp chat etc.

THE MOST COMMON SUBJECT LINES TO REAL LIFE PHISHING EMAILS GLOBALLY ARE:

Google: You were mentioned in a document; "Strategic Plan Draft"
HR: Important: Dress Code Changes
HR: Vacation Policy Update
Adobe sign: Your Performance Review; Password Check Required Immediately; Acknowledge Your Appraisal

Phishing is becoming more and more popular among cyber criminals:

Approximately **1.2%** of all emails sent globally are phishing attempts. **81%** of organisations worldwide have seen an increase in email phishing attacks. Phishing scams contribute to almost **36%** of all data breaches, as reported by Verizon's 2022 Data Breach Report.

Fraudulent websites vs phishing scams: same but different

Fraudulent websites are illegitimate online platforms designed to deceive visitors into providing personal or financial information through deceptive means, often by mimicking trustworthy entities.

Phishing scams, on the other hand, involve fraudulent practices, such as misleading emails or communication, in which attackers masquerade as reputable sources to trick individuals into revealing sensitive information.

Safe internet browsing is similar to safely walking through busy streets. The principles of vigilance, awareness, and proactive measures against risks, ingrained in our everyday physical safety habits, find resonance in the digital world.

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

1. Similar to physical habits, digital practices become second nature with practice.
2. Be cautious of phishing scams and fraudulent websites.
3. Verify the authenticity of websites before sharing personal information.
4. Utilise security tools, update browsers, and employ strict privacy settings.
5. Regularly update operating systems, browsers, and security software.

> It is now a safer online world for you and everyone around you

TEST YOUR KNOWLEDGE

Which of the following email subjects are commonly associated with phishing emails? (Select all that apply):

1. Your account has been compromised. Verify now!
2. Urgent: Immediate action required for payroll update
3. Newsletter subscription confirmation
4. Free gift! Click to claim your prize
5. Important: Review and approve document
6. Security alert: Unusual login activity detected
7. Congratulations! You've won a lottery.

The answers can be found in the last chapter: Cyber Answers

Public wifi: A haven for cyber intruders

Pro tip:

If you are not willing to scream it from the rooftops, don't share it on a public wifi network.

Malika enjoys a delightful dinner with her best friend Leyla at their favourite restaurant, catching up after not having seen each other for a while. They are enjoying a lively conversation, exchanging personal anecdotes and recounting their summer adventures. The chat transitions to discussing work, as they are planning to collaborate on a shared project.

In the course of their conversation, Malika and Leyla exchange private information about the location of shelters they have established to host women who are survivors of gender based violence. They discuss how to help residents, making plans to visit the next day.

Now, envision a scenario where the entirety of this conversation becomes public knowledge; everyone in the restaurant is listening in on them.

While that might feel like an exaggeration, it illustrates the vulnerability of public wifi networks. Each user on the network gains unrestricted access to transmitted information.

Connecting to a wifi hotspot grants the hotspot owner the authority to monitor online activities, and in some instances even track physical movements.

Consider the implications when working from a cafe, using a work computer to handle sensitive information, exchange emails or share confidential details. All of this data becomes visible and accessible on the public wifi network, turning it into a potential playground for hackers.

CHRIS LIVERANI | UNSPLASH

If you need to view some sensitive information or access a password protected accounts, there are some safe methods:

1. Set up and use a hotspot
When accessing sensitive information or password-protected accounts, setting up a personal hotspot can enhance security. Follow these steps:

a. Activate hotspot:
- On your smartphone, navigate to settings.
- Find the "Hotspot" or "Tethering" option.
- Turn on the hotspot and set a strong password.

b. Connect devices:
- Connect your computer or other devices to the hotspot.
- Ensure your hotspot is password-protected for an added layer of security.

c. Access sensitive data:
- Once connected, safely view sensitive information or access password-protected accounts.

Note: These are general guidelines and might differ depending on your device and operating system.

SPOTLIGHT

Although convenient, public wifi poses many risks

Cybercriminals can intercept data between your device and the wifi router, potentially capturing sensitive information.
Lack of encryption means data transmitted over public wifi is more vulnerable to interception.
Cyber attackers may set up rogue wifi hotspots with deceptive names, tricking users into connecting to malicious networks.
Hackers can use packet sniffing tools to capture and analyse data packets, extracting sensitive details.

2. Use a VPN (Virtual Private Network)
Utilising a VPN is an effective way to secure your online activities, especially on public wifi. Here's a quick guide for Windows and Mac:

a. Select a VPN provider:
- Choose a reputable VPN service and sign up for an account.

b. Download and install:
- Download the VPN client for your operating system.
- Install the software following the provided instructions.

c. Connect to a server:
- Launch the VPN application.
- Choose a server location and establish a secure connection.

d. Access sensitive information:
- With the VPN active, safely access sensitive information on public networks.

Note: These are general guidelines and might differ depending on your device and operating system.

3. Wait until you can use a trusted non-public wifi network
When dealing with highly sensitive data, the safest option might be to wait until you have access to a non-public wifi network that you trust. Avoiding public networks altogether eliminates the risks associated with them.

Remember, the security of your data is paramount, and choosing the right method depends on the level of sensitivity and urgency.

WHAT'S A VPN?

VPN, or Virtual Private Network, is your digital cloak of invisibility. With VPN, your data wears an encrypted disguise, making it as secure as a secret agent on a classified mission.

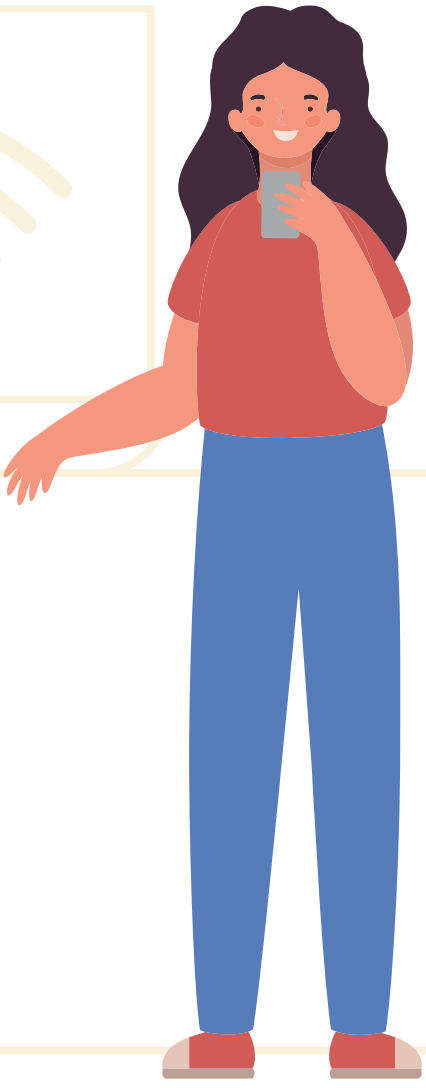
SPOTLIGHT

Choosing a VPN provider, what to consider

Security and privacy features: Ensure the VPN has robust encryption, a no-logs policy and advanced security protocols to safeguard your data.
Server network and locations: : A diverse and widespread server network enhances your online experience. Choose a VPN with servers strategically located worldwide.
Connection speed: Opt for a VPN that provides fast and reliable connection speeds, crucial for seamless browsing and streaming.
Features and performance: Evaluate the additional features offered by the VPN, such as kill switches, split tunnelling and overall performance.
Pricing: While a free VPN might seem tempting, paid services often provide better security and performance. Choose a VPN that fits your budget and offers value for money.

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

1. Public wifi networks expose users to potential cyber intruders as each user on the network has unrestricted access to transmitted information.
2. When dealing with highly sensitive data, waiting for access to a trusted, non-public wifi network is the safest option.
3. Consider setting up and using a hotspot or VPN.
4. Choosing the right security method depends on the level of sensitivity and urgency.



TEST YOUR KNOWLEDGE

Question 1: What potential risks do public wifi networks pose?
A. Limited access to information
B. Enhanced security
C. Exposure to cyber intruders
D. Physical tracking of users

Question 2: How does a VPN enhance security on public wifi?
A. By exposing sensitive information
B. By limiting online activities
C. By establishing a secure connection
D. By avoiding public networks

The answers can be found in the last chapter: Cyber Answers

What do your house keys and passwords have in common?

> Passwords are like underwear: you don't let people see it, you should change it very often, and you shouldn't share it with strangers
>
> CHRIS PIRILLO

Pro tip:
Avoid using the same password across multiple accounts.

One afternoon as she walks through the bustling streets of the city, Leyla encounters an unexpected crisis – she realises that she has misplaced her keys. Panic sets in as she fears that her physical security might be compromised. As well as leaving her home vulnerable to theft, Leyla does not now feel secure sleeping at home. Swiftly, Leyla retraces her steps and scours the streets, but can't find her keys. So recognising the severity of the threat, Leyla promptly contacts the police, reports the missing keys, calls a locksmith to change the lock and requests multiple copies of the keys, leaving one with someone she trusts.

Now, consider this: just as Leyla's keys open the door to her home, passwords act as the keys to digitally valuable items—bank accounts, emails, communication, private information, work data, beneficiaries, personal communication, etc.

Amount of time to crack a password	
7 characters	.29 milliseconds
8 characters	1 – 5 hours
9 characters	11 hours – 5 days
10 characters	3 – 4 months
11 characters	1 decade
12 characters	2 centuries

Source (5) https://www.verveit.com/blog/is-your-password-strong-enough

LEVON DARBANYAN | UNSPLASH

Your quick guide to establishing strong and secure passwords

Avoid common passwords
Steer clear of easily guessable passwords like "password123" or common words. Opt for unique combinations to enhance security.
Good example: Tr3ndyP@ssw0rd! (Complex and unique)
Bad example: Password123 (Simple and commonly used)

Use a mix of characters
Incorporate a combination of uppercase and lowercase letters, numbers and special characters to increase complexity.
Good example: F!reDraGon87#
(Includes a variety of character types)
Bad example: password1234
(Lacks diversity and complexity)

Length matters
Create long passwords as they are generally more robust. Aim for at least 12 characters.
Good example: S3cur3L0ngP@ssw0rd!
(Long and complex)
Bad example: ShortPwd!
(Too brief to provide strong security)

Unique for each account
Avoid using the same password across multiple accounts. Unique passwords for different platforms enhance overall security.

Avoid personal information
Steer clear of incorporating personal details like names, birthdays or addresses. This information is easily accessible and can be exploited by attackers.
Good example: B3l0v3dPet#R0v3r
(Incorporates personal elements but not obvious)
Bad example: JohnsDog123
(Directly related to personal information)

Regularly update passwords
Change passwords periodically to reduce the risk of compromise. Set reminders to update them every few months.

Set Up 2FA (two-factor authentication) or MFA (multiple factor authentication): Two-factor authentication (2FA) adds an extra layer beyond just passwords, requiring users to provide a second form of identification such as a temporary code sent to their mobile device.

This significantly reduces the risk of unauthorised access, even if passwords are compromised.

Use a password manager
If you have many accounts and need to keep track of all your passwords, use a password manager. Choose a reliable password manager: here are some of the safest password managers recommended by cyber experts.

1Password:
Known for its feature-rich and intuitive design.
Expert recommendation: Considered the best overall password manager, offering a balance of features, intuitiveness, and affordability.

Bitwarden
Open-source password manager with a strong emphasis on security.
Expert recommendation: Recognised for its security measures and the ability to deploy it across various platforms.

NordPass
Developed by the creators of NordVPN, offering robust security features.
Expert Recommendation: Noted as one of the top choices for password management in 2024.

Consider using a passphrase
A passphrase is a sentence like string of words used for authentication that is longer than a traditional password, easy to remember and difficult to crack.
Good example: PurpleElephant$JumpHigh (Long and memorable passphrase)
Bad example: MyPassword123 (Simple and still resembles a common password)

PASSWORD OR PASSPHRASE?

A password is typically a combination of characters, including letters, numbers, and symbols, used to authenticate a user. It is usually shorter and more complex.

On the other hand, a passphrase is a longer sequence of words or a sentence. It tends to be more natural to remember but longer in length.

Which is Safer? The safety of a password or passphrase depends on various factors, including length and complexity. Generally, longer and more complex passwords or passphrases are safer. Passphrases often provide better security due to their length and the use of natural language elements.

Number of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2 bn years	48 bn years	380 bn years
18	6 days	481k years	126 bn years	2 tn years	26 tn years

Source (6): https://tech.co/password-managers/how-long-hacker-crack-password

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

1. Both house keys and passwords are critical for security, with compromises posing risks to physical and digital safety.
2. Use strong passwords or passphrases to protect your accounts. Use unique combinations, a mix of characters, and longer passwords (at least 12 characters) to enhance security.
3. Implement additional security measures like Two-Factor Authentication (2FA) to add an extra layer of protection beyond passwords.

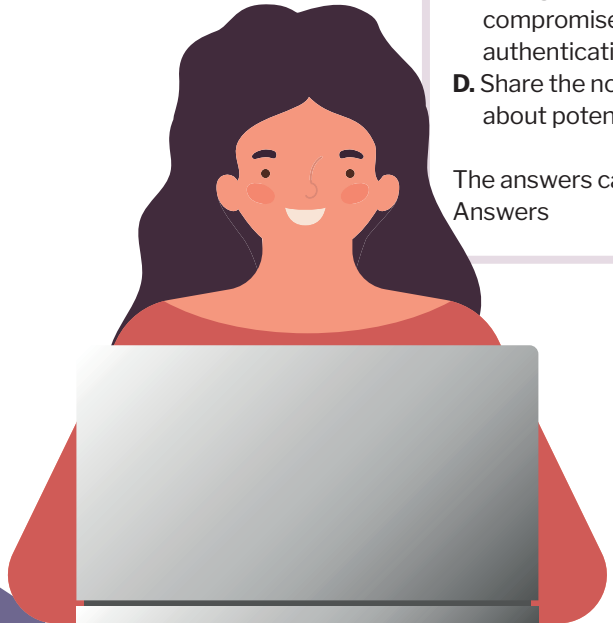
TEST YOUR KNOWLEDGE

Scenario: Malika receives a concerning notification about unauthorised access to personal information in a data breach. Panicked, she realises the need to take immediate steps to address the situation and safeguard sensitive data.

Test question:
What steps should Malika take after receiving the notification about unauthorised access in a data breach?

A. Ignore the notification; it might be a false alarm.
B. Contact the company involved and demand an explanation.
C. Change passwords associated with the compromised account and enable two-factor authentication.
D. Share the notification on social media to warn others about potential risks

The answers can be found in the last chapter: Cyber Answers

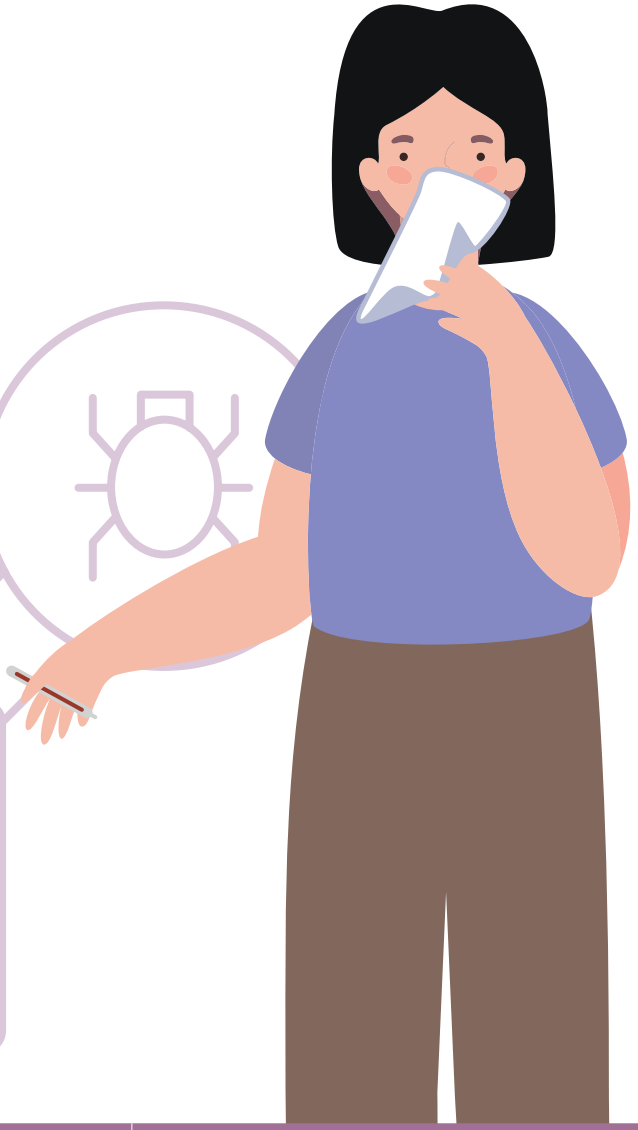


Malware: A virus that weakens your computer's immune system

It's Monday morning, and Leyla is getting ready to conduct a two-day training for young activists in her city advocating for women's rights on social media and in their communities. However, an unexpected adversary emerged – a virus. A nasty bug infiltrates her body, leaving her feeling sick, feverish and weak.

As the virus takes hold, Leyla's immune system springs into action. White blood cells, the defenders of her body, rally to identify and neutralise the threat. But meanwhile, Leyla's energy rapidly wanes, impacting her ability to carry out her key role. Unable to conduct the training, she postpones it until her immune system manages to neutralise the virus.

Something similar happens when malware infiltrates your computer, compromising files and slowing down functionality.



WHAT IS THE DIFFERENCE BETWEEN MALWARE AND VIRUS?

Malware is a broad term encompassing any malicious software designed to harm a computer or network. It includes various types like viruses, trojans and ransomware. On the other hand, a virus is a specific type of malware that replicates itself and spreads to other files or systems. In essence, all viruses are malware, but not all malware is a virus.

Aspect	Malware on Computer	Virus in Human Body
Nature	Malicious software designed to harm or exploit systems.	Infectious agents causing illness in living organisms.
Forms	Various forms, including viruses, worms, Trojans, etc.	Different viruses causing diseases (e.g., influenza).
Transmission	Spreads through infected files, websites, or downloads.	Transmitted through direct contact, droplets or air.
Replication	Replicates within the computer system to spread further.	Replicates within the host's cells to spread illness.
Intent	Can lead to data theft, system disruption, or espionage.	Causes diseases, with varying degrees of severity.
Detection	Detected by antivirus software and cybersecurity tools.	Diagnosed through medical tests and examinations.
Prevention	Prevented by using antivirus, firewalls, and updates.	Prevented by vaccinations, hygiene, and immune health.
Impact on system	Slows down, disrupts operations, or damages data.	Causes symptoms ranging from mild to severe illness.
Treatment	Requires malware removal tools and system restoration.	Medical treatments, medications, and supportive care.
Evolution	Constantly evolving with new variants and techniques.	Evolves through mutations, leading to new virus strains.
Origin	Developed by cybercriminals or malicious entities.	Originates from natural sources or may be produced by humans

Malware is short for malicious software

(YES, THEY HAVE NICKNAMES TOO!)

It is a collective term for various harmful programs designed to harm computers, steal information, or disrupt normal functioning.

At this point, you might be thinking why would cyber criminals target you or your organisation with malware?

1. **Political espionage:** Hackers may engage in political espionage to gather intelligence on women involved in political affairs and human rights, exploiting organisations' sensitive data (7).
2. **Disruption of activism:** Malicious actors may aim to disrupt the activities of women's rights groups by infecting their systems with malware. This can hinder their ability to advocate for change.
3. **Gaining foothold for larger attacks:** Hackers often use initial malware infections to gain a foothold within a network. Once inside, they may expand their access and launch more extensive attacks, potentially compromising the organisation's entire infrastructure (8).
4. **Political or social agendas:** Threat actors may deploy malware to promote specific political or social agendas, such as spreading misinformation or discrediting the activities of women's rights organisations (9).

Malika eventually went to the doctor, took the recommended treatment and recovered from the virus. She ended up giving the training a few days later and made sure to mention the importance of cyber safety for any activist, peacebuilder and advocate.

SO DOES THAT MEAN THAT THERE ARE OTHER TYPES OF MALICIOUS SOFTWARE? YES, QUITE A FEW...

Spyware: Like digital spies, quietly observing and stealing information

Adware: Like annoying pop-up salespeople, bombarding you with unwanted ads.

Ransomware: Like a digital kidnapper, locking your files until you pay a ransom.

Worm: Like spreading infections, self-replicating and exploiting vulnerabilities.

Trojan: Like deceptive gifts, masquerading as legitimate software.

Cyber expert approved antivirus, anti-spyware, and firewall solutions:

Bitdefender®

norton™

A few numbers about different types of malware:

Globally, **72.7** per cent of all organisations fell prey to a ransomware attack in 2023, highlighting the significant impact on cybersecurity.

In 2020, **61** per cent of organisations experienced malware activity spreading from one employee to another; by 2021, this number rose to **7** per cent, emphasising the increasing frequency of malware incidents.

Adware accounted for **25.28** per cent of all mobile threats detected in 2022, indicating its prevalence as a prominent type of threat.

Sources
(10) https://www.cobalt.io/blog/cybersecurity-statistics-2024
(11) https://www.comparitech.com/antivirus/malware-statistics-facts/
(12) https://terranovasecurity.com/blog/cyber-security-statistics/

WHAT IS A FIREWALL?

A firewall is like a security guard for your computer network.

- It monitors and controls the traffic coming in and going out, acting as a protective barrier.
- It lets in the good stuff and blocks the bad stuff, such as cyber threats.
- Firewalls can be either hardware or software and play a crucial role in maintaining a secure online environment.

SPOTLIGHT

How to protect yourself (we mean your computer) against malware?

Beside using strong passwords, and avoiding clicking on suspicious links, here are a few but important things you should do:

- Install trusted antivirus and anti-spyware programs to detect and eliminate malware threats.
- Keep software updated: that includes operating systems, applications and antivirus software.
- Use a firewall to monitor incoming and outgoing network traffic and act as an additional barrier against malware.

TEST YOUR KNOWLEDGE

Question 1: What is the primary purpose of spyware?
A. Enhancing system performance
B. Observing and stealing information
C. Locking files until a ransom is paid
D. Spreading infections and self-replicating

Question 2: Why might cybercriminals engage in political espionage using malware?
A. To enhance system performance
B. To disrupt activism
C. To gain a foothold for larger attacks
D. To promote specific political or social agendas

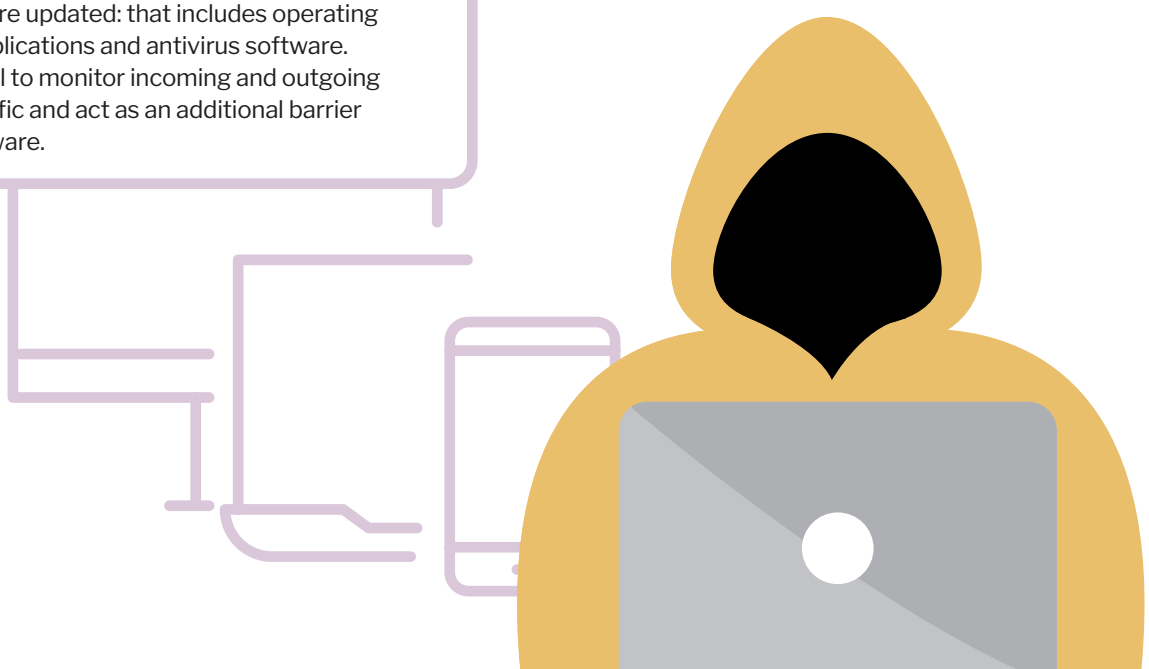
The answers can be found in the last chapter: Cyber Answers

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

Leyla's battle against a virus mirrors the impact of malware on computers, both disrupting normal operations and causing a slowdown in functionality. Malware is an umbrella term for various forms of harmful software.

Cybercriminals target activists with malware for political espionage, activism disruption, promotion of specific political and social agendas and as an entry point for larger attacks.

Stay safe by installing antivirus and anti-spyware programs, keep software updated and use a firewall.



Secure your devices, your organisation and your beneficiaries

The journey to cyber safety can be challenging. Changing habits can take time and work but is paramount to safeguard sensitive information, protect yourself, your colleagues and most importantly your beneficiaries.

This guide aims to provide practical steps for securing devices, fostering awareness and implementing robust cybersecurity measures within the organisation.

GETTING STARTED: CHANGING CYBER HABITS STEP BY STEP

1. Employee training
- Conduct cybersecurity awareness sessions to familiarise employees with common threats, phishing attacks and the importance of secure online behaviour.
- Start with basic concepts before delving into more complex cybersecurity practices.

2. Regular refresher sessions
- Schedule periodic cybersecurity refresher sessions to reinforce knowledge and update employees on emerging threats.
- Encourage open communication, allowing employees to share concerns and ask questions.

3. Phased implementation
- Introduce cybersecurity measures in phases to avoid overwhelming employees.
- Begin with fundamental practices such as password hygiene and gradually progress to more advanced measures.

> To be effective, cybersecurity training should result in changed behaviour

BEHAVIOURAL CHANGES FOR ENHANCED CYBER SAFETY

In addition to technical measures, fostering behavioural change is vital for a resilient cybersecurity posture:

1. Safe browsing habits
- Advise employees to scrutinise URLs, avoid clicking on suspicious links, and verify the legitimacy of websites.
- Implement web filtering tools to block access to malicious sites.

2. Two-factor authentication (2FA)
- Promote the use of 2FA to add an extra layer of protection to accounts and systems.
- Encourage the adoption of biometric authentication for enhanced security.

3. Incident reporting culture
- Encourage a culture where employees feel comfortable reporting any suspicious activities or security incidents promptly.
- Establish a clear incident response plan for efficient resolution.

By prioritising cybersecurity, women's rights organisations can fortify their digital defences and protect their invaluable work. A combination of education, phased implementation and fostering behavioural changes will contribute to a resilient and secure cyber environment.

ANRAS VAS | UNSPLASH

IMPLEMENTING CYBERSECURITY MEASURES ON AN ORGANISATION LEVEL

1. Installing antivirus software
- Utilise reputable antivirus software to detect and eliminate malicious threats.
- Regularly update antivirus databases to stay protected against the latest threats.

2. Regular software & hardware updates
- Regularly update operating systems and applications to patch vulnerabilities.
- Enable automatic updates whenever possible to ensure timely protection against known exploiters.
- Ensure that all hardware components, including routers and IoT devices, have the latest firmware updates to address security issues.

3. Using firewalls
- Enable firewalls on both individual devices and network infrastructure.
- Configure firewalls to monitor and control incoming and outgoing network traffic, enhancing overall security.

4. Setting up permissions for employees
- Implement the principle of least privilege, granting employees only the necessary permissions for their roles.
- Regularly review and update permissions to align with organisational changes and employee roles.

5. Using encryption
- Encourage the use of encryption for sensitive communications and data storage.
- Implement end-to-end encryption for messaging platforms to protect confidential conversations.

6. Regular backups
- Emphasise the importance of regular data backups to mitigate the impact of ransomware attacks or data loss.
- Store backups securely, preferably in an offline or cloud environment, and test restoration processes periodically.

TEST YOUR KNOWLEDGE

Question: What is the primary aim of cyber security training?
A. Enhancing device aesthetics
B. Resulting in changed behavior
C. Ignoring cybersecurity measures
D. Focusing only on complex practices

Question: What is the recommended approach for implementing cyber security measures on an organisational level?
A. Immediate implementation of advanced measures
B. Introducing measures randomly
C. Phased implementation starting with fundamental practices
D. Relying solely on employee permissions

Question: Which cyber security measure involves granting employees only the necessary permissions for their roles?
A. Encryption
B. Firewalls
C. Regular backups
D. Setting up permissions

The answers can be found in the last chapter: Cyber Answers

IF YOU TAKE AWAY A COUPLE OF CRUCIAL POINTS FROM THIS SECTION, LET IT BE THESE:

1. Leyla's battle against a virus mirrors the impact of malware on computers, both disrupting normal operations and causing a slowdown in functionality.
2. Malware is an umbrella term for harmful software that comes in various forms.
3. Cybercriminals target activists with malware for political espionage, activism disruption, entry point for larger attacks, and promotion of specific political and social agenda.
4. Stay safe by installing Antivirus and Anti-spyware programs, keep software updated and use a firewall.

SCENARIO EXERCISE: PHISHING SIMULATION AND PRIORITY RESPONSE

Simulate a sophisticated phishing attack targeting employees to assess the organisation's ability to detect, respond, and prioritize cyber security actions.

Exercise steps:

1. Phishing email simulation:
- Send realistic phishing emails to randomly selected employees.
- Craft scenarios that mimic common phishing tactics, such as urgent requests, enticing offers or disguised as internal communications.

2. Employee responses:
- Observe how employees respond to the phishing emails.
- Assess whether they recognise the phishing attempt, report it promptly or fall victim to the attack.

3. Security team notification:
- Notify the cyber security team about the simulated phishing attack.
- Evaluate the team's response time and efficiency in analysing and confirming the phishing attempt.

4. Incident response priority:
- Based on the severity of the phishing attack, assign priorities to incident response actions.
- Test the organisation's ability to prioritize and allocate resources effectively.

5. Communication and training:
- Communicate the simulated incident to employees, emphasising the importance of vigilance against phishing threats.
- Provide targeted training on recognising and reporting phishing attempts.

6. Post-exercise analysis:
- Conduct a thorough analysis of the exercise, identifying areas for improvement.
- Evaluate the effectiveness of the organisation's cybersecurity training and adjust priorities accordingly.

This scenario exercise focuses on prioritising responses to phishing attacks, a prevalent cybersecurity threat. It helps organisations gauge their readiness to address evolving security challenges.

> In cyber security, you can have the best protection (anti-virus, VPN etc…) and that might still be not enough. People are the weakest link. One human mistake can cause the protection system to fail
>
> DAVIT GHONGHADZE, CYBER SECURITY EXPERT

A few last words

As we conclude this cyber resilience guide, tailored for women's rights organisations, the crucial intersection between digital security and the advocacy for human rights should be crystal clear. Safeguarding sensitive information and digital assets are not just best practice; they are an essential prerequisite for the pursuit of human rights.

The evolving landscape of cyber threats underscores the urgency for women's rights organisations to cultivate a paradigm shift in behaviours. Robust cybersecurity measures, encompassing real-time monitoring and proactive solutions, are imperative to fortify digital infrastructure against potential risks.

In an ideal world, individuals like Leyla and Malika could dedicate themselves entirely to advocating for women's rights, leading grassroots initiatives and conducting training without the looming concern of cyber threats. However, the reality of our world necessitates a parallel advocacy – one for cybersecurity changes and the integration of safer practices at the organisational level.

Picture Malika and Leyla, unwinding at their favourite restaurant after a demanding week. Having conducted a thorough cyber assessment and received training on prioritised cybersecurity measures, they now feel empowered to safeguard their teams as well as their beneficiaries.

This guide is not intended to instil fear; rather, it stands as a practical resource, arming women's rights organisations with the knowledge and tools essential for securely navigating the digital landscape. By doing so, they can concentrate on their pivotal mission of advancing gender equality and human rights.

SINCERLEY MEDIA | UNSPLASH

Your cyber answers

Chapter: Am I really a target?

The correct answer is A
Targeted attack to steal her data. By identifying an organisation Leyla collaborates with and pretending to represent them to send her an email, it means that cyber hackers have done their research and targeted Leyla specifically. By asking her to update her credentials, they were aiming to steal her username and password and hack her accounts.

Chapter: Safe Internet Browsing - Would you walk on a busy street with your bag open?

Answer: The correct answers are 1, 2, 4, 5, 6, 7. The only wrong answer is 3. While an email with the subject 'Newsletter Subscription Confirmation' can be the title of a phishing email, all other email subjects have a sense of urgency and use fear to prompt immediate action. This emotional manipulation is a common tactic employed by hackers to deceive individuals into clicking on phishing email links.

Chapter: Public wifi - A Haven for Cyber Intruders

Answer to question 1 is C
Exposure to cyber intruders. The most significant risk that public wifi networks pose is exposing you to cyber intruders. In some cases, this exposure allows them to track your physical movements.

Answer to question 2 is C
By establishing a secure connection. VPN enhances security on public wifi by redirecting your internet connection through a private server, making your real IP address inaccessible and hiding your online activity.

Chapter: What do your house keys and passwords have in common?

Answer to the scenario test question is C
Change passwords associated with the compromised account and enable two-factor authentication. If her password was compromised and leaked in a data breach, it means cyber hackers have access to her username and passwords. Malika should promptly change the password of the compromised account and activate two-factor authentication for an extra layer of protection.

Chapter: Malware - A virus that weakens your computer's immune system

Answer to question 1 is B
Observing and stealing information. The primary purpose of spyware is similar to that of digital spies – to quietly observe and steal information.

Answer to question 2 is B
To disrupt activism. Hackers may engage in political espionage to gather intelligence on activists, peacebuilders and organisations, exploiting sensitive data to disrupt activism.

Chapter: Secure your devices, your organisation, and your beneficiaries

Answer to question 1 is B
Resulting in changed behaviour. The primary aim of any cybersecurity training is to encourage people to change their behaviour in a way that contributes to a safer work environment for all employees in the organisation.

Answer to question 2 is C
Phased implementation starting with fundamental practices. The recommended approach is to start one step at a time starting with the fundamentals such as safe internet browsing, recognising phishing emails. You can then move on to encrypted emails, firewalls, VPNs and other more complicated topics.

Answer to question 3 is D
Setting up permissions.

Sources

https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations

https://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma

https://www.amnesty.org/en/latest/campaigns/2015/08/how-governments-are-using-spyware-to-attack-free-speech/

https://tech.co/password-managers/how-long-hacker-crack-password#:~:text=A%2010%2Ddigit%20password%20that,hacker%20up%20to%20two%20weeks

https://www.verveit.com/blog/is-your-password-strong-enough/

https://www.cobalt.io/blog/cybersecurity-statistics-2024

https://www.comparitech.com/antivirus/malware-statistics-facts/

https://terranovasecurity.com/blog/cyber-security-statistics/

https://www.linkedin.com/pulse/breaking-down-tactics-used-hackers-exploit-womens-rights-middle

https://www.sciencedirect.com/science/article/pii/S245195882200001X

https://www.ibm.com/topics/threat-actor

https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights

https://www.coe.int/nb/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR

iwpr.net

IWPR Moldova
Mediacor building,
Alexei Mateevici 60 str.,
MD-2009,
Chișinău

IWPR United Kingdom
48 Gray's Inn Road,
London WC1X 8LT
Tel +44 (0)20 7831 1030

IWPR United States
1156 15th Street NW Suite 505,
Washington, DC 20005
Tel +1 202 393 5641

IWPR Netherlands
Almaatsweg 7,
7856 TJ Benneveld,
Netherlands
iwpr-nl@iwpr.net