Inclusive Cybersecurity - Brief

Strategies to ensure an accessible and safe digital experience

G3ict
The Global Initiative for Inclusive ICTs
Advancing the Rights to Digital Access for Persons with Disabilities

CONTENT

I. Introduction

Inclusive cybersecurity, a pivotal and dynamic field, is vital in safeguarding all individuals and communities from cyber threats, irrespective of their background, identity, or resources.

This brief will cover how to safeguard vulnerable groups around cybersecurity; however, **a specific focus will be placed on accessibility and security for people with disabilities**.

According to the Cybersecurity and Infrastructure Security Agency (CISA), cybersecurity is not just a set of technologies but a practice. It is the art of protecting networks, devices, and data from unauthorized access or criminal use and ensuring confidentiality, integrity, and availability of information. This practice involves implementing technologies, processes, and measures to secure digital systems and information from hacking, phishing, malware, ransomware, and other cyber threats. Cybersecurity is essential for safeguarding sensitive information, ensuring the integrity and availability of systems, and maintaining privacy in the digital world.

To ensure a safe, inclusive digital environment, every stakeholder, including you, must understand their roles and shared responsibilities. This collective effort is crucial in understanding the potential vulnerabilities of networks, devices, and users, especially the most vulnerable users.

Why should you put Inclusive Cybersecurity on your organizational radar?

- **Equity and Fairness:** Ensures no one is left vulnerable due to lacking resources or support.
- **Broader Protection:** Helps to secure a more comprehensive range of individuals and organizations, reducing the overall risk of cyber threats.
- **Improved Solutions:** Diverse perspectives contribute to more innovative and effective cybersecurity solutions.
- **Preparedness:** Widespread education and training help individuals and organizations better respond to and mitigate cyber threats.

II. Vulnerable Groups: Your Customer, Your Employees!

One of the primary vulnerable groups that need to be considered is people with disabilities, which can include parts of the aging population. Ensuring cybersecurity for people with disabilities involves several key safeguards to address their unique needs. Risks of discrimination, exclusion from online content or services, and exploitation can play significant concerns for people with disabilities. People with disabilities may encounter inaccessible websites or technologies, limiting their ability to participate fully online. They may also be targets of ableist abuse or scams designed to exploit their disabilities.

Ensuring cybersecurity for people with disabilities involves several fundamental safeguards to address their unique needs. Here are some essential measures:

1. **Accessible Technology:** Ensure all cybersecurity tools and platforms are accessible. This includes screen readers for visually impaired users, voice recognition software, and other assistive technologies.
2. **Inclusive Policies:** Develop and implement cybersecurity policies that consider the needs of people with disabilities. This includes training staff to support users with disabilities and ensure all communications are accessible.
3. **Education and Awareness:** Provide education and resources tailored to people with disabilities to help them recognize and avoid cyber threats like phishing and malware.
4. **Strong Authentication Methods:** Use multi-factor authentication (MFA) accessible to all users. For example, offering options beyond text-based codes, such as biometric authentication.
5. **Regular Audits and Updates:** Conduct regular audits of cybersecurity measures to ensure they remain accessible and effective. Update systems and protocols as needed to address new threats and accessibility challenges.
6. **Collaboration:** Governments and technology companies should work together to create standards and guidelines that ensure cybersecurity measures are inclusive and accessible.

These steps can help create a safer digital environment for everyone, including those with disabilities.

Is there a specific area of cybersecurity you're particularly interested in?

Box 1: Accessibility and Security

Challenges: Security features like CAPTCHA, password protections, and two-factor authentication can pose significant difficulties for users with disabilities, such as those with visual or cognitive impairments.

Equitable Access: Security measures should provide equal access to all users. For instance, CAPTCHAs should have accessible alternatives like audio or logic-based challenges.

User Experience: The user experience should remain intuitive and seamless, ensuring that security features do not frustrate or exclude users with disabilities.

Customization: Security solutions should be adaptable to different user needs, allowing for customized authentication methods that align with individual abilities.

Best Practices:

Accessible CAPTCHAs: Implementing accessible alternatives to traditional visual CAPTCHAs, such as audio CAPTCHAs or logic puzzles.

Clear Communication: Providing clear and accessible instructions for security processes, ensuring users understand the steps and can easily complete them.

Testing with Users: Involving users with disabilities in the testing phase to identify and rectify accessibility issues in security features.

Other Vulnerable Users Groups

1. **Children and Adolescents Risks:** Cyberbullying, online predators, exposure to inappropriate content, privacy violations, and identity theft. Concerns: Young users may need more maturity to recognize or respond to dangers online. They are also more susceptible to manipulation and may share personal information without understanding the consequences.
2. **Elderly Individuals Risks:** Scams, phishing attacks, identity theft, and misinformation. Concerns: Older adults may not be as familiar with technology, making them easier targets for fraud. They might also need help to differentiate between credible and non-credible sources of information.
3. **Women and Gender Minorities Risks:** Harassment, cyberstalking, non-consensual sharing of intimate images, and gender-based violence. Concerns: Women and gender minorities often face targeted attacks and abuse online, which can lead to psychological harm, privacy violations, and physical threats.

4. **Migrants and Refugees Risks:** Misinformation, exploitation, and scams. Concerns: Migrants and refugees might face language barriers and lack awareness of digital safety practices, making them vulnerable to online fraud, misinformation, or targeted harassment.
5. **Low-Income Individual Risks:** Exploitation, scams, and limited access to digital resources. Concerns: Economic disadvantage can limit access to secure devices, reliable internet, and digital literacy education, increasing vulnerability to online threats.

III. Protective Measures

Some of the primary areas of concern around inclusive cybersecurity include digital literacy programs and online communities. There are protective measures that can be used for projects.

Government's Role in Digital Literacy Programs. Digital literacy programs, which focus on safe online behavior, recognizing scams, and understanding privacy settings, are not just about protection. They empower vulnerable groups, giving them the tools and knowledge to navigate the digital world confidently. Governments can play a crucial role by implementing stronger regulations to protect vulnerable users, including stricter penalties for online harassment and exploitation. Online platforms, on the other hand, can contribute by enforcing these regulations and creating a safer online environment for all users.

Online Communities Support Systems. Online communities are more than just a collection of users. They support vulnerable groups where abusive behavior is reported, resources are offered, and inclusive environments are fostered. This sense of shared responsibility and connection makes these communities so powerful. They also provide guides, videos, and tutorials in accessible formats, such as captions, transcripts, sign language interpretation, and simplified versions for people with cognitive disabilities, further strengthening this sense of community.

Organizations should promote cybersecurity workshops that include inclusive dynamics, allowing people with different types of disabilities to participate actively. These workshops should contain information to help persons with disabilities identify fake emails, messages, and websites. It is essential to provide clear and accessible examples to avoid falling victim to scams, considering that people with disabilities will be browsing the internet in different ways (visually, auditorily, and with the help of assistive technologies).

Other important tips to protect vulnerable groups from cybersecurity threats include:

- Automatic, accessible reminders to remind you to update passwords, activate antivirus protection, and adopt other secure habits. These reminders are not just about keeping your digital life safe. They are a constant source of reassurance and support, ensuring you never forget to take the necessary precautions.
- When using mobile applications, recommend using apps that are not only secure but also accessible. Ensuring end-to-end encryption is enabled means that only the sender and the recipient can read the messages and privacy settings are appropriately configured is essential. When choosing communication apps, verify they are compatible with screen readers or other accessibility tools.
- Ensure people know how to adjust their privacy settings on social media to limit who can see their information. Many online tutorials are available in accessible formats, including captions, sign language interpretation, and simplified text versions. Users should familiarize themselves with tools to report and block accounts in case of harassment, ensuring these functions are easy to access and use.
- Developing accessible guides on what to do if a security breach occurs, including support contact numbers and transparent steps to mitigate damage, is crucial to supporting vulnerable groups. Ensuring that technical support services have accessible options like video calls with sign language interpretation or chat responses adapted for screen readers provides reassurance and support, making technology a security facilitator rather than a barrier.

IV. Malicious Software (Malware)

Malware, short for malicious software, is crafted to take over or disrupt a victim's computer systems. These programs often disguise themselves as harmless files or links, tricking users into downloading them and thereby granting unauthorized access to the victim's computer and potentially the entire organization's network.

Box 2: Types of malicious software

Backdoor: refers to a method of bypassing normal authentication procedures to gain unauthorized access to a system or network. It is a type of malicious software or code that creates a hidden entry point, allowing attackers to access or control the system remotely without the user's knowledge.

Malwares: short for "malicious software," refers to any software intentionally designed to cause harm to computers, networks, or devices.

Ransomware: type of malicious software designed to block access to a victim's files or system until a ransom is paid. It typically encrypts the victim's data or locks them out of their system, rendering it inaccessible. The attacker then demands payment in exchange for a decryption key or access credentials to restore the affected files or system.

Trojan: type of malicious software that disguises itself as a legitimate or benign program to deceive users into installing it. Trojans can cause significant damage by compromising system security and facilitating further malicious activities.

Viruses: type of malicious software that attaches itself to legitimate programs, files, or system boot sectors to execute harmful actions when the infected software or file is run. The primary goal of a virus is to cause damage or disruption by infecting as many files or systems as possible.

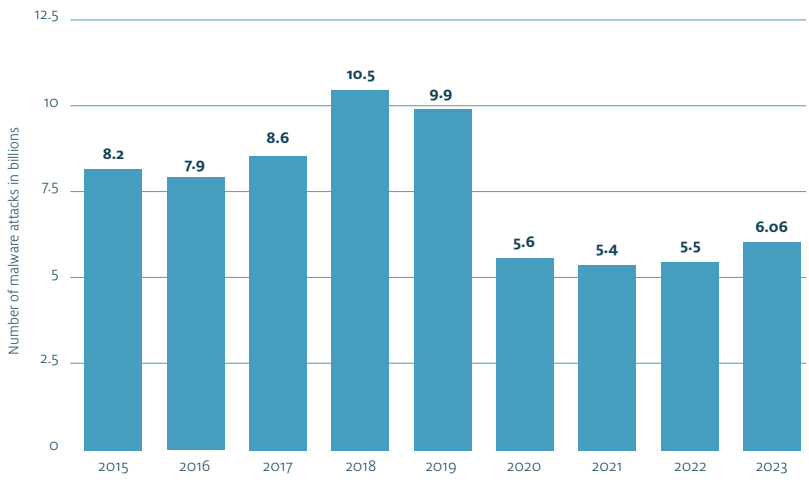
Worms: type of malicious software designed to replicate itself and spread to other computers or networks without requiring user interaction. Unlike viruses, which attach themselves to legitimate programs or files, worms operate independently and often exploit vulnerabilities in operating systems or software to propagate. Worms can cause significant damage by rapidly infecting large numbers of systems and disrupting network operations.

In 2023, 6.06 billion malware attacks were detected globally, with the majority occurring in Asia-Pacific. The most frequently blocked types of malware included worms, viruses, ransomware, trojans, and backdoors. Among the two primary attack vectors—email and websites—websites were more commonly used for phishing attacks.

Phishing attacks, with significant financial impacts, remain a major cause of data breaches. In 2022 alone, the FBI's Internet Crime Complaint Center (IC3) received nearly 800,944

phishing complaints [1], leading to losses exceeding $10.3 billion. The trend of targeting Software as a Service (Saas) users and social media platforms also continues, with attacks on platforms like LinkedIn and Zoom being prevalent

Chart 1. The annual number of malware attacks worldwide from 2015 to 2023 (in billions)



Source: Details: Worldwide; SonicWall; 2015 to 2023; data is based on SonicWall Capture Labs characteristics; wider industry metrics may vary. Statista 2024

With around 30 percent of adults worldwide encountering phishing scams in 2022, it's clear that proactive measures are more crucial than ever. According to the Anti Phishing Working Group (APWG[2]) 1st Quarter 2024 Phishing Activity Trends Report[3], during the fourth quarter of 2022, there were over 1.35 million unique phishing sites worldwide.

Box 3: Phishing: type of cyber-attack where malicious actors attempts to deceive individuals into disclosing sensitive information, such as usernames, passwords, credit card numbers, or other personal data. This is typically done by masquerading as a trustworthy entity in electronic communications, such as emails, text messages, or fake websites.

Inclusive cybersecurity challenges

- **Resource Disparities:** Not all communities have equal access to cybersecurity resources and education.
- **Representation:** Cybersecurity fields often need more diversity, limiting the scope of problem-solving and innovation.
- **Complexity:** Balancing inclusivity with the technical complexities of cybersecurity can be challenging.

1 2022 Internet Crime Complaint Center (IC3) Annual Internet Crime Report. https://www.iafci.org/app_themes/docs/Federal%20Agency/2022_IC3Report.pdf

2 https://apwg.org/

3 Link to the APWG Report: https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf

Critical Aspects of Inclusive Cybersecurity

When addressing essential aspects of inclusive cybersecurity, it is vital to understand the problems and invest in solutions. Below are highlighted problems matched up with possible solutions to consider.

1. **Problem: Accessibility:** Designing cybersecurity tools and resources that people with varying levels of ability use.

Solution. Tools. The solutions involve tools that include creating software with accessible interfaces for people with disabilities and ensuring that cybersecurity training is available.

2. **Problem: Equitable Protection:** Ensuring all communities, especially marginalized or underserved groups, receive adequate protection from cyber threats.

Solution. Resources and Support. The solution involves addressing disparities in access to cybersecurity resources and support.

3. **Problem: Diverse Perspectives:** Encouraging diversity in cybersecurity teams to bring different perspectives and approaches to solving security challenges.

Solution. Diverse Teams. Diverse Teams will identify a wider range of threats and develop more comprehensive solutions.

4. **Education and Training:** Providing cybersecurity education and training to a broad audience, including underserved communities. This can help build a more knowledgeable and prepared public.

Solution. Professional Certifications. Providing employees with a professional certification focusing on disability and inclusion can elevate and benchmark education and training initiatives.

5. **Policy and Regulation:** Advocating for policies and regulations that promote fairness and equity in cybersecurity practices includes addressing issues like data privacy and the ethical use of technology.

Solution. Focus Groups. Provide opportunities for employees with diverse backgrounds to provide feedback through focus groups and engagement feedback sessions.

V. Moving Forward

To advance inclusive cybersecurity, efforts must focus on creating accessible tools, promoting diversity in the field, ensuring equitable protection for all, and providing comprehensive education and training. This holistic approach strengthens individual and organizational security and fosters a more resilient and equitable digital environment.

Contributors

Authors

Monica Duhem, PhD
Director Global Advisory Network, G3ict

Christopher M. Lee, Ph.D.
G3ict CEO

Spanish Translation for the IAAP Mexican Chapter

Luz María Servín
Director of Fundación Hearcolors

References

National Institute of Standards and Technology (NIST). (n.d.). NIST Special Publication 800-63: Digital Identity Guidelines.
Retrieved from https://pages.nist.gov/800-63-3/sp800-63-3.html

CrowdStrike. (2024). 2024 Global Threat Report.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

Internet Crime Complaint Center (IC3). (2022). 2022 Annual Internet Crime Report. Federal Bureau of Investigation.

Anti-Phishing Working Group (APWG). (2024). 2024 Phishing Activities Trend Report.