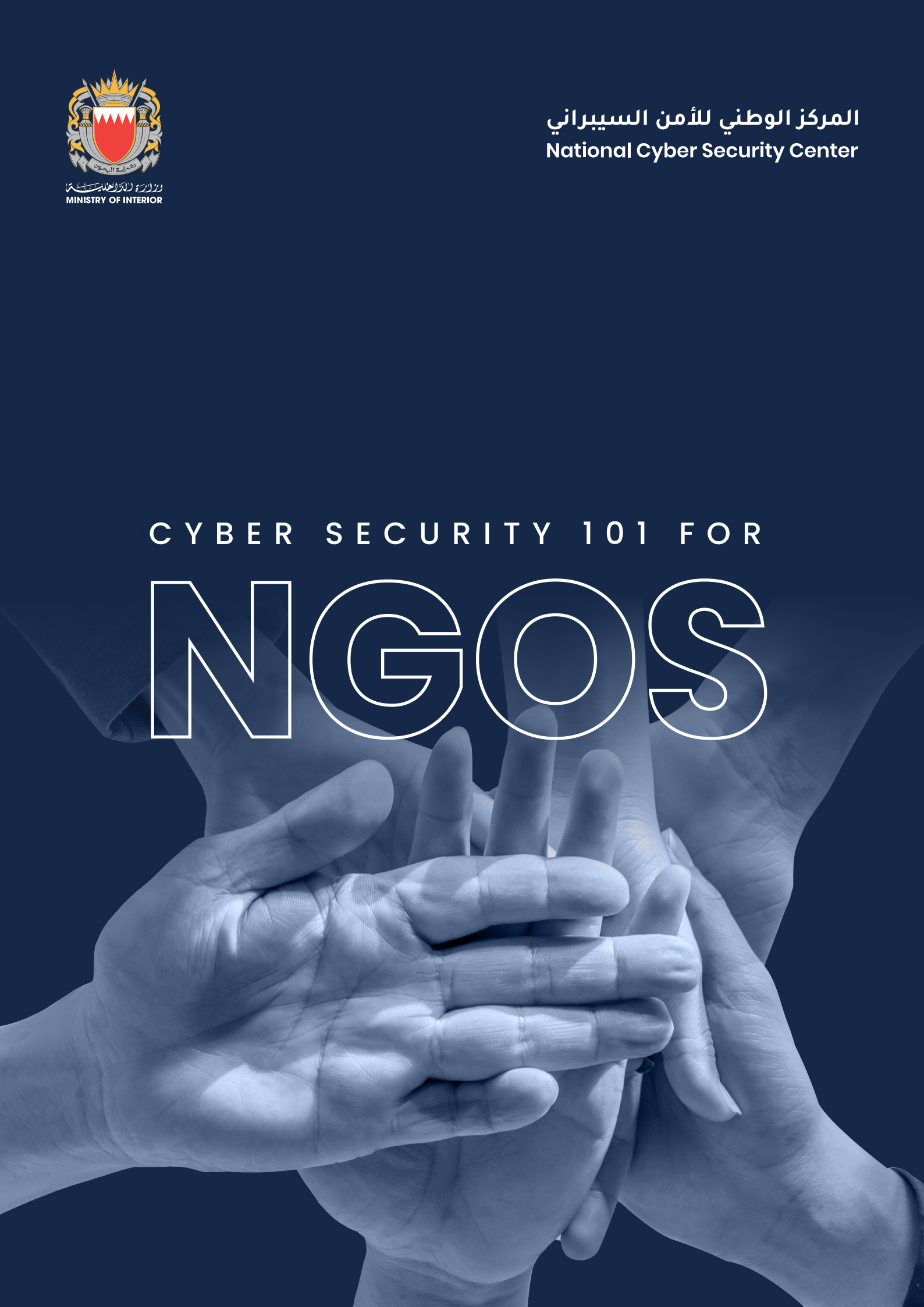
وزارة الداخلية
MINISTRY OF INTERIOR

المركز الوطني للأمن السيبراني
National Cyber Security Center

CYBER SECURITY 101 FOR NGOS



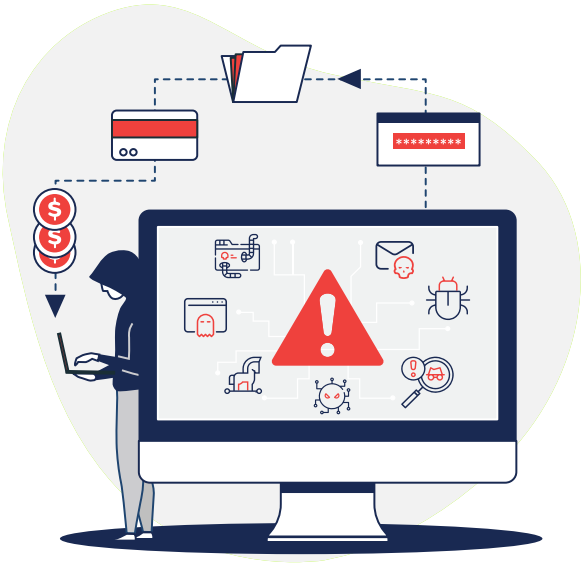
Index

Why NGOs Need Cyber Security

Many institutions worldwide have started working with NGOs to stop cyberattacks and disruptions caused by cyber threats.

This resulted in a global response to the international call for collective action against cyber threats and attacks on humanitarian nonprofit and non-governmental organizations (NGOs).

Cyber researchers observed that most nation-state actors continue to focus operations and attacks on (NGOs) for various objectives, one of which is Fraud.
It usually combines spear phishing and identity theft to deceive NGOs into completing wire transfers.

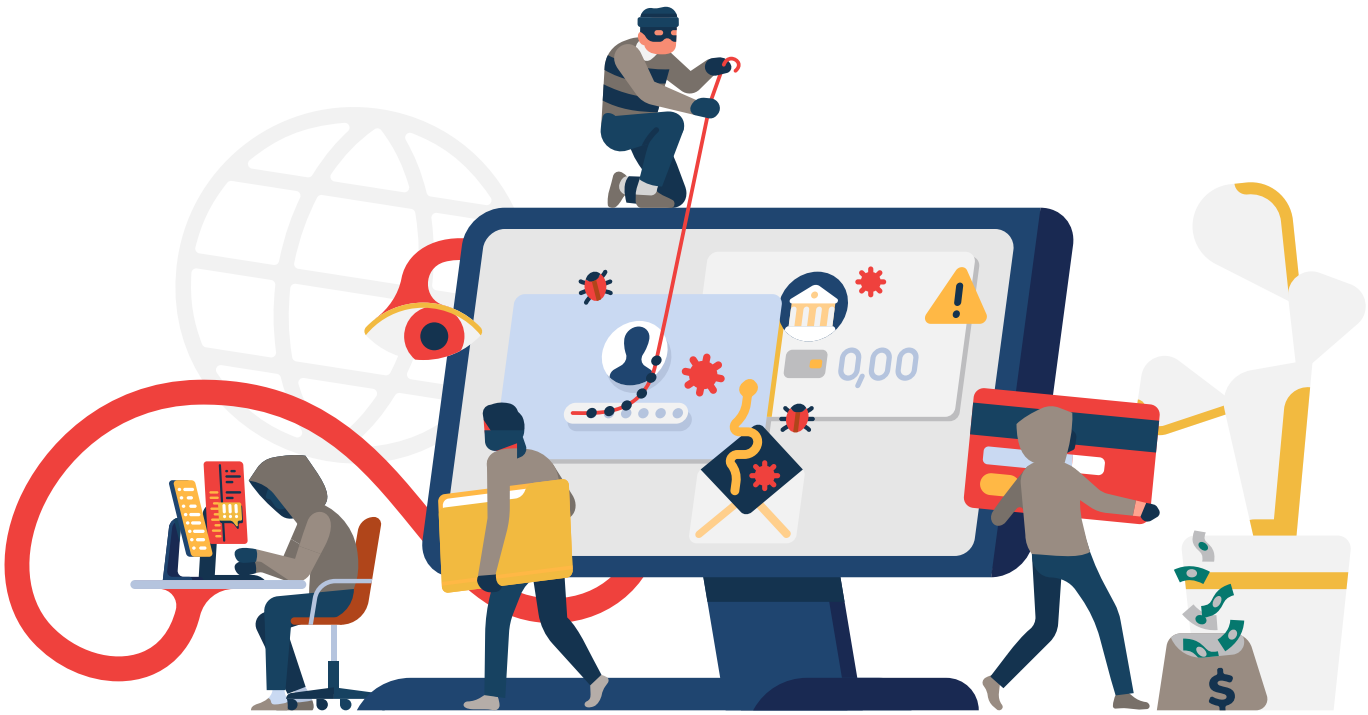


As part of a hacking strategy known as CEO Fraud, fraudsters create fake business email addresses and assume the identities of executives or reliable workers to dupe them into authorizing unlawful wire transfers of money.

Another type of attack is ransomware for financial gain, where an attacker encrypts crucial data in a computer system, some of which risks getting destroyed. As a result, organizations have no choice but to pay a ransom.

In a nutshell, cyberattacks on NGOs may be carried out for the following reasons:

1. Preventing them from carrying out their activities.
2. Gaining access to data on beneficiaries and other stakeholders.
3. Stealing funds, data, and financial information.
4. Use stolen data in disinformation campaigns.
5. Use the organization's infrastructure to attack and perform malicious activities online and hold it accountable, due to identified cybersecurity vulnerabilities.



Numerous cyberattacks occur because hackers exploit weaknesses in systems or because of 'Human Error'.

Although attacks are getting more sophisticated, not every NGO can afford to hire dedicated cyber security staff. Non-Governmental Organizations (NGOs) should invest in Cybersecurity Awareness trainings and follow best practices to make their organizations more resilient to cyber attacks.

RISKS

Ransomware

Web defacement

Data interception

Whaling Phishing Attacks (CEO Fraud)

Misusing identities because of identity theft

INCREASE YOUR ORGANIZATION'S PREPAREDNESS

AGAINST CYBER-ATTACKS

Increase Cybersecurity Awareness in Your Organization

Cyber security is a shared responsibility. Invest in awareness programs for your employees and IT staff. Educate your staff through conducting training sessions and providing awareness materials to increase data and technology hygiene and ultimately, making cyber security a part of your organization's culture.

Protect Critical Data

Secure the data of employees and beneficiaries against potential data theft risks and take extra measures in protecting data relating to funds and NGO projects. Encryption and Masking are 2 key methods to consider implementing.

Ensure That Critical Data and Systems Have Regular Backups

Backing up critical data is an essential process. Make sure to have the right policy and technical measures in place, such as having multiple copies of encrypted critical data; this way, it is easier to restore if an attack occurs.
Inquire about the backup procedures used by any third-party databases and services if used in the organization and check the documentation to see if you can periodically download a copy of your data.

Strengthen Your Passwords and Use Multi-Factor Authentication

Create passwords adhering to security standards for each system you use. Wherever applicable, use multi-factor authentication (MFA) as a second layer of security.
If you have difficulty remembering multiple passwords, use a trusted password manager to securely store them.

Install and Keep Anti-virus Software Up-To-Date

Anti-virus software should be installed and kept up to date on every machine in the organization. Keeping your anti-virus software up-to-date can help prevent malware from infecting your machine or network if a user clicks on an infected link.

Be Cautious When Choosing Service Providers

Anti-virus software should be installed and kept up to date on every machine in the organization. Keeping your anti-virus software up-to-date can help prevent malware from infecting your machine or network if a user clicks on an infected link.

Consider Cyber Insurance

Look into getting cyber insurance for your organizations. Depending on the coverage, it could be inexpensive and helpful if your organization ever gets breached. This insurance can cover the costs of reputational damage and recovery and other potential consequences of a breach.

Use Encrypted and Secure Websites

Technology has made it easier for charities and nonprofits to accept donations online, but it has also made it easier for hackers to steal during financial transactions that are in session. Using trusted, encrypted, and secure websites during online financial wire transactions help in keeping information safe for users and the organization. Do not ignore the notifications about unsafe websites or dangerous & deceptive content your browser sends you.

Look Out for Phishing and Ransomware Attacks

It's easy to get in touch with donors and customers through emails. Automated emails and newsletters inform interested parties of what's happening at your organization. Still, you could be at risk if a malicious link is clicked on, or suspicious files are downloaded. Always, verify the sender's email address to ensure the email comes from a reliable source and make sure to verify suspicious links or files in the email before clicking or downloading them.

Secure Your Platforms and Financial Transactions

NGOs use various in-built or online platforms for donations and fund-raising events.
A good donation platform should use encryption like SSL or TLS. This will secure any checkout processes as well as encrypt any entered information. 2FA's like OTPs and secure codes are necessary to implement to keep donors safe. Look for a donation platform that offers multi-factor authentication to secure donors and users data.

Ensure Your Email Communications Are Secure and Reliable

There are certain risks involved when sending emails containing private documents or financial data. This is since most emails sent are not well protected while in transfer between servers. Donor information may be collected, organized, and transmitted securely if you use a secure email server and encrypted network.

Install Security Solutions

Make sure your organization has security solutions like firewalls, email gateways, and intrusion detection and prevention systems to safeguard sensitive data, systems and employees.

Monitor Volunteers' Activities

Volunteers give their time for a variety of reasons, such as wanting to support the community where they might have access to sensitive data from your organization. Even though most volunteers have good intentions, there are a few bad actors who may volunteer their time to gain access to your sensitive data. Ensure that you keep an eye on volunteer activity because bad actors sometimes manage to slip through the loopholes, putting your organization at risk of a cyberattack.

Managing Human Risks

Human risk, if managed in an efficient manner, can help your organization reduce costs and save time in defending against cyber-attacks. This can be achieved by identifying risks and changing behaviors in your organization instead of solely relying on technologies and solutions. By turning people into human sensors, you can improve your organization's response and resilience capabilities.

Stay Up-To-Date With Latest System and Software Version

Keep up-to-date with updates and security patches. It's important to operate using the latest versions to be less susceptible to hacks and exploits. That might just be effective to protect you from Zero-Days!

SCAN ME

Refer to the **Baseline Cyber Security Controls** on our website on our website for information on the core set of cybersecurity controls that organizations should implement in order to meet protection requirements for risk management.

Quick tips:

- Protect critical data by taking regular backups.
- Install and keep anti-virus software up-to-date.
- Increase organizational awareness of cyber security.
- When doing online financial activities like wire transfers, ensure you use encrypted and secure websites.
- Beware of ransomware and phishing scams.
- Strengthen your passwords and use multi-factor authentication.
- Consider using cyber insurance.
- Be cautious when choosing your IT service providers.
- Secure your email communications by encrypting sensitive emails.
- Monitor suspicious volunteers' activities.
- Ensure that your organization has security solutions such as firewalls, email gateways, and IDS/IPS to aid in the detection and prevention of cyber-attacks.
- Manage human risks by investing in awareness and education on cyber security risks.

WITH REGARDS

NATIONAL CYBER SECURITY CENTER

وزارة الداخلية

MINISTRY OF INTERIOR

www.ncsc.gov.bh

#CyberWiser