General Principles of Digital Safeaty

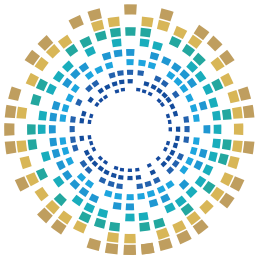
Digital Safety in Diplomacy

Target Group:
Diplomats

Teacher's Booklet

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

General Principles of Digital Safety

Digital Safety in Diplomacy

Target Group

Diplomats

Teacher's Booklet

Intellectual Property Rights

This material is owned by the National Cyber Security Agency in the State of Qatar, and all intellectual property rights, including copyright and publishing rights, are wholly owned by the National Cyber Security Agency in the State of Qatar.

Therefore, all rights are reserved for the Agency, and no part of this material may be reproduced, quoted, copied, transmitted, or distributed, in whole or in part, in any form or by any means, whether electronic or mechanical, including but not limited to photocopying, recording, or using any information storage and retrieval system, whether currently existing or developed in the future, without prior written approval from the Agency.

Any unauthorized use or reproduction of this material shall subject the violator to legal action under applicable laws.

Dear Participant,

With rapid technological advancement and the expansion of the internet into every aspect of life, cybersecurity threats now affect all sections of society. Accordingly, raising awareness of digital safety concepts has become a strategic necessity, as it is the principal means of protecting society against these threats.

As part of the National Initiative for Digital Safety's efforts to improve digital safety standards across society, this booklet, published by The National Cyber Security Agency, provides diplomats with practical guidance to enhance digital protection both personally and professionally.

Contents	Page number

Introduction

In an era of rapid digital transformation, digital safety is no longer optional; it is now fundamental to the security of states, their institutions and their personnel, particularly in the diplomatic work environment, which relies on the exchange of sensitive information, communication through digital channels, and the management of negotiation files in cyberspace, an open domain marked by pervasive cybersecurity threats.

This booklet is intended to raise awareness of digital safety among diplomats and staff of diplomatic missions abroad and to enhance their capability to protect data, devices and correspondence against potential cybersecurity threats. It also aims to equip them to use modern technologies safely and effectively, which are now integral to everyday diplomatic practice.

Chapter One

Protection of Data and Devices

Protecting data and information in the diplomatic work environment is primarily a national responsibility, as overseas missions and embassies rely on technology for communication and for managing sensitive documents. Accordingly, awareness of digital safety is essential to securing correspondence and protecting state secrets in cyberspace.

First: The Concept of Cybersecurity and Its Objectives

Cybersecurity is the framework for protecting systems, networks and information against cyber threats, including attacks, intrusion attempts and data exfiltration.

Importance of Cybersecurity

Securing official channels of communication, including email and virtual platforms.

Ensuring the confidentiality of information and the integrity of data

Protecting systems and networks from unauthorised monitoring and intrusion attempts.

Cybersecurity Objectives

01
Protecting sensitive information against unauthorised access or disclosure.

02
Ensuring continuity of operations.

03
Enhancing diplomats' capability to manage cybersecurity risks.

04
Enhancing international trust in digital diplomacy

Did you know?

Did you know that Cyber Diplomacy is an emerging field that aims to develop internationally agreed norms of behaviour in cyberspace[(1)].

1. Diplomacy in Cyberspace, American Foreign Service Association, on site: https://afsa.org/diplomacy-cyberspace?utm_source=chatgpt.com.

Second: Device Protection

Digital devices, particularly smartphones, are essential to diplomatic work, enabling communication, the exchange of official correspondence and day-to-day file management. However, if not properly secured, these devices can become a primary entry point for cybersecurity threats.

To protect devices, particularly smartphones, adopt the following preventive measures[2]:

1

Regularly update the operating system and applications to patch security vulnerabilities that attackers may exploit.

2

Enable two-factor authentication (2FA) on all accounts, including email, to prevent unauthorised access even if passwords are compromised.

3

Use strong, unique passwords that include a mix of uppercase and lowercase letters, numbers and symbols, and change them regularly.

4

Install trusted security software, including antivirus and security scanners, and keep it up to date.

2. Cybersecurity Best Practices, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices.

5

Avoid installing applications from unofficial sources or clicking on unknown links, as this may expose you to spyware.

6

Switch off the camera and microphone when not in use, as some malware may activate them remotely without the user's knowledge.

7

Encrypt sensitive data and files on the device and enable automatic locking when the device is left unattended or idle.

8

Avoid using public or open Wi-Fi networks, particularly in airports, hotels and cafés, as such networks are prime environments for data interception.

Third: Digital Safety During Travel

Travel is one of the situations in which devices and data are most exposed to cybersecurity risks, particularly when attending conferences or international meetings, or when using foreign networks that may be insecure.

Before, during and after travel, diplomats should take preventive measures to protect data and devices, including:

Pre-Travel Measures

- Run comprehensive security scans on devices to confirm they are free from malware and unauthorised applications.
- Carry out a temporary factory reset of mobile devices, retaining only essential data.
- Back up sensitive files using encryption.
- Before travelling, enable two-factor authentication (2FA) on all official accounts.

Measures During Travel

- Avoid using public or free Wi-Fi networks.
- Avoid plugging personal devices into public USB charging points.
- Avoid downloading or installing new applications or opening links from unknown or untrusted sources while travelling.

Post-Travel Measures

- Clear cached data and temporary files from devices used during travel.
- Change the passwords of all accounts used while travelling.
- Review official email accounts for any unusual activity.

Caution!

Avoid using public Wi-Fi or plugging personal devices into public USB charging points, as this could compromise your device's security[3].

3. What is ‹Juice Jacking› and Tips to Avoid It, Federal Communications Commission, on site: https://www.fcc.gov/juice-jacking-tips-to-avoid-it

Fourth: Protection of Data and Documents

Protecting data and documents is a key element of digital safety and requires the adoption of practices that keep information secure and confidential, whether at rest or in transit.

Key practices include

1. Using strong encryption (AES-256) to protect sensitive files; they may only be opened or read with cryptographic keys authorised by the relevant official authority[4].

2. Storing important documents on closed internal networks (intranets) rather than on public cloud services to minimise the risk of compromise or unauthorised disclosure.

3. Implementing the principle of least privilege by granting access and modification rights to files only to personnel authorised in accordance with their grade and role within the mission.

4. Implementing digital rights management (DRM) controls to prevent unauthorised printing, copying or sharing of official files[5].

4. How to Protect the Data that is Stored on Your Devices, CISA, on site: https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices

5. Digital Rights Management (DRM), FORTINET, on site: https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm

5 Maintaining encrypted backups of important data in separate locations so that they can be restored if the originals are lost or damaged.

6 Using encrypted, password-protected external storage devices (USB drives or external hard drives), not leaving them unattended in public places, and not connecting them to untrusted devices.

7 Monitoring access and modification of sensitive files through audit logs that record every action performed on those files.

Did you know?

Did you know that phishing and social engineering are the most common methods attackers use to steal credentials, typically by deceiving users into disclosing sensitive information or downloading malware[6].

6. What is incident response? IBM, on site: https://www.ibm.com/think/topics/incident-response

Chapter Two

Cybersecurity Incident Management

The diplomatic working environment is inherently vulnerable to cybersecurity risks; every electronic message, administrative system, and communication channel represents a potential vector for a cybersecurity incident. Therefore, understanding the nature of these incidents and the mechanisms for responding to them is a fundamental component of ensuring operational continuity and safeguarding against any sudden digital threat.

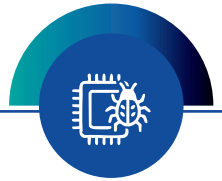
First: Cybersecurity Incidents

A cybersecurity incident is defined as any adverse event that compromises the confidentiality, integrity, or availability of systems and information within the digital working environment. This incident may arise from human error, a technical malfunction, or a deliberate attack intended for espionage, sabotage, or extortion.

Such incidents include

A breach of diplomatic email, and the subsequent theft or leakage of official correspondence.

Malware and ransomware attacks.



Spear phishing, which targets specific members of staff.

Manipulation of media content or official data, such as the dissemination of falsified information.

Attacks on communications systems or official websites.

Second: Responding to Cybersecurity Incidents

Processes and techniques for the detection of, and response to, cyber threats, security breaches, or cyberattacks. A formal incident response plan enables cybersecurity teams to mitigate or prevent damage[7].

7. What is incident response? IBM, on site: https://www.ibm.com/think/topics/incident-response

The Importance of Incident Response

1. Mitigate losses by rapidly isolating compromised systems to prevent the spread of the attack.
2. Protect reputation by controlling the situation and preventing the leakage or dissemination of sensitive information.
3. Provide accurate digital evidence to be used subsequently to identify the source of the attack and assess the threat level.
4. Ensure the continuity of operations through contingency plans that enable the team to continue tasks without disruption.
5. Enhance the cybersecurity framework by reviewing existing procedures and incorporating lessons learned after each incident.

Did you know?

Did you know that the use of artificial intelligence in cybersecurity can help detect sophisticated attacks, such as phishing and targeted attacks, before they cause significant damage[8].

8. Cyberattacks, IBM, on site: https://www.ibm.com/think/topics/cyber-attack#498277090

Third: Role and Responsibilities of the Diplomat

In the event of a cybersecurity incident, every diplomat becomes an essential part of the response framework. An employee›s actions in the initial moments can determine the extent of the damage or the success of the technical team in controlling the situation.

Responsibilities During an Incident

1. Immediately report any unusual activity in email, on devices, or on the internal network, and refrain from attempting to resolve the issue independently.

2. Avoid opening or clicking suspicious files or links, even if they appear to have been sent by an official authority or a colleague.

3. Digital evidence, such as messages, logs, or compromised files, must not be deleted or modified, as these elements are critical to subsequent investigation and analysis.

4. Full cooperation must be extended to the Cybersecurity Team by providing all necessary information and sharing observations, including the precise timings at which the anomaly was detected.

5. Adherence to instructions issued by the Technical Team is mandatory, such as immediately isolating the device from the network or promptly resetting passwords upon request.

6. The confidentiality of the incident must be strictly maintained, and it shall not be discussed on social media platforms or outside official channels, in order to prevent the dissemination of rumours or media exploitation of the situation.

Chapter Three

Cyber Threats and Preventive Measures

Cyber threats are escalating on a daily basis, becoming increasingly sophisticated and highly targeted, particularly against sensitive sectors such as diplomatic operations. Current attacks are no longer indiscriminate; rather, they are meticulously engineered to gather precise intelligence or to influence political and economic positions.

First: Types of Cyber Threats

The diplomat is considered one of the foremost targets for cyberattacks globally, owing to the sensitivity of the information they handle and the critical nature of the decisions informed by it.

Types of Cyber Threats

Spear Phishing

This is considered the most prevalent method employed against diplomats, whereby deceptive, official-looking emails containing malicious links or attachments are dispatched. Once opened, the attacker gains the capability to access credentials or operational systems[(9)].

Identity Spoofing

This relies upon the imitation of diplomats› official email accounts or credentials to deceive other parties, or to dispatch fabricated messages in their name; this action risks the leakage of information or the creation of crises within official communication channels[(10)].

Deepfake

This entails the deployment of fraudulent content or falsified data to undermine the reputation of diplomatic missions or to sow political discord between states.

Did you know?

Did you know that Multi-Factor Authentication (MFA) significantly reduces the likelihood of account compromise[(11)].

9. What is spear phishing? IBM, on site: https://www.ibm.com/think/topics/spear-phishing.

10. Spoofing and Phishing, FBI, on site: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing.

11. Multifactor Authentication, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.

Cyber Threat Prevention

1. Multi-Factor Authentication (MFA) must be enabled for all official accounts and email systems to ensure protection, even in the event of password compromise.
2. Verify the identity of the sender and the content before interacting, by scrutinising all links and attachments and contacting the sending entity via an alternative channel to confirm authenticity.
3. Digital signatures and certificates must be utilised in all official correspondence to distinguish authentic from fraudulent email and prevent identity impersonation.
4. Continuous training must be provided for diplomats and staff on the methodologies of Phishing, Deepfake, and Social Engineering to ensure the rapid acquisition of early detection capability.
5. Reliance must be placed on deepfake detection tools and technologies to analyse suspicious digital content before it is disseminated or officially addressed.
6. Clear institutional security policies must be enforced, encompassing regular system updates, the encryption of sensitive data, and the immediate reporting of any suspicious activity to enable rapid incident response.

Caution!

Sensitive data that is unencrypted or insufficiently protected is susceptible to exploitation or theft.

Second: Malware

Malicious software (Malware) is considered one of the most serious tools deployed by attackers to compromise systems or conduct espionage against users. These are programs specifically engineered to inflict damage upon devices, steal data, or achieve remote control over systems.

Types of Malicious Software[12]:

Viruses

It spreads from one file to another, gradually infecting the system and causing data corruption or degraded performance. It often spreads through attachments or removable storage media.

Ransomware

It encrypts important files on the device and then demands a ransom from the victim to decrypt them.

Trojans

They may appear to be useful programs or legitimate files, but in reality they grant attackers covert access to the target device.

Spyware

It operates in the background without the user›s knowledge, collecting data, correspondence, and images, and logging keystrokes.

12. Viruses vs. Ransomware & Malware: Types and Explanation, CISCO, on site: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virus-vs-ransomware-malware.html

Malicious Software Prevention

Install and maintain the continuous updating of reputable security software.

Do not open any files or links from unknown sources.

Only secure networks must be utilised, and connection to public or open networks is to be avoided.

Conduct routine device inspections to detect any unusual activity or suspicious files.