<Security Awareness cover example>

Summary

Introduction

Research suggests that human error is present in 90% of information leakage cases. This guide aims to raise awareness among <COMPANY NAME> employees and consequently reduce the risk of data losses, information leaks, penalties, business and resource losses, and, especially, the risk of damage to the company's image and reputation.

The issues presented in this guide address common errors observed in the daily activities of employees in any company, such as those related to email access, internet browsing, improper use of external devices, among others.

Therefore, we have included mandatory rules in this document that must be followed by all employees working with company equipment and/or in their digital environments, as well as recommendations for best practices to enhance the security of our technological environment. <COMPANY NAME> will continuously monitor compliance with the rules and recommendations presented here.

In addition to this Information Security Best Practices Guide, intended for knowledge and application by all company employees, <COMPANY NAME> also has an Information Security Policy with technical definitions to be implemented by its information security team.

TOP 10

The main precautions related to information security on <COMPANY NAME> equipment and digital environment:

Mandatory

- Create strong passwords: Passwords should be at least 12 characters long, combining letters, numbers, and special characters.
- Keep the operating system, applications, and software up to date.
- Protect computers from viruses/malware: Therefore, every <COMPANY NAME> device must have the antivirus software defined by the company installed.
- Regularly back up important files.
- Enable Two-Factor Authentication: This feature requests a second verification at the time of login, preventing access to accounts even when the password is leaked.

Best Practices

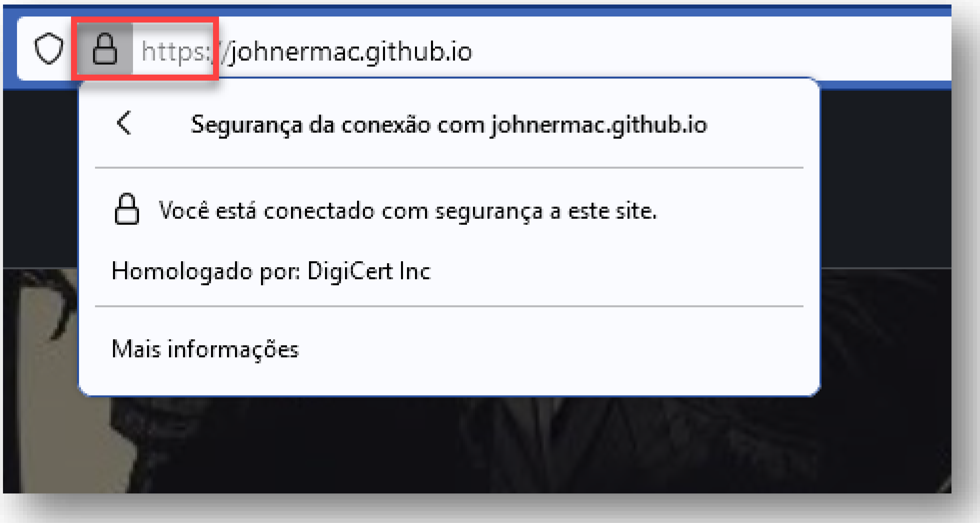
- Remove unnecessary programs/files.
- Do not leave the computer unlocked when absent: Always lock the screen of your device when leaving your workstation.
- Avoid using external devices (USB, external hard drives, smartphones) on <COMPANY NAME> equipment: They can also spread viruses.
- Authorize remote access only for the <COMPANY NAME> IT department.
- Do not use file-sharing software: This increases the risk of malicious files and attacks (BitTorrent, uTorrent, Deluge, etc.).

Web Browsing

Mandatory

- Do not download files from sources not permitted by the antivirus or the information security team.
- Use only the browsers authorized by <COMPANY NAME>, which includes: Firefox, Chrome, Edge, Brave, Safari, or Opera.
- Never save passwords/accounts in browsers.
- Verify if the website you are accessing is HTTPS; you can check if the padlock icon is in the address bar. The "S" in HTTPS stands for Secure, indicating that the site implements SSL encryption.

Example:



https://johnermac.github.io

Segurança da conexão com johnermac.github.io

Você está conectado com segurança a este site.

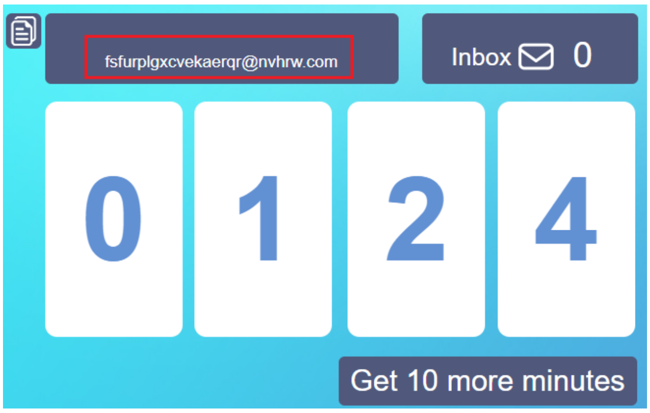
Homologado por: DigiCert Inc

Mais informações

- Pay attention when clicking on links and downloading. If they seem suspicious, do not click.
- Check weekly if the browser is up to date. Preferably, enable automatic updates.
- Enable the option to clear your data when exiting the browser.
- Do not save confidential information without encryption on private cloud services (Google Drive, Dropbox, iCloud, etc.).
- Only enable the option requesting information about your location if extremely necessary.
- Emails with free offers or advertisements often contain viruses. Do not click on the indicated buttons and/or links.
- Avoid accessing public Wi-Fi networks. It is very easy to capture information during transmission on a network with no protection.
- The use of a VPN is recommended for cases that require extra security.

Suggestions

If you need to provide an email for a quick registration, the quickest and safest way to do so is through the website [10 Minute Mail](). This service allows you to create a disposable email that lasts for 10 minutes. This prevents you from using your actual email for registrations, serving as a way to avoid spam.



fsfurplgxcvekaerqr@nvhrw.com

It is possible for pop-ups to appear while browsing certain domains. Stay vigilant and avoid clicking on them. It is recommended to activate the "AdBlock" extension in browsers; it is an ad blocker that will help mitigate this issue.

[AdBlock: How to Install in your Browser]()

Passwords

The most common way for unauthorized individuals to gain access to your information is through password guessing. Nowadays, there are various techniques for executing this malicious practice. We will discuss the key precautions in this chapter:

Mandatory

- Create strong passwords with a minimum of 12 characters, combining letters, numbers, and special characters.
- All passwords should be changed within 3 to 6 months.
- Never reuse old passwords.
- Do not store your passwords in files (Notepad, Excel, Word, etc.).
- Do not share your passwords with anyone.
- Always use different passwords for each account/service. Using identical passwords increases the risk of exposure, as if one site is hacked, all other accounts become vulnerable.
- Enable Two-Factor Authentication (2FA) as determined by the <COMPANY NAME> administrative area. There are various options for the second verification, such as a smartphone, SMS, email, biometrics, token (Examples: Google Authenticator, Microsoft Authenticator, Authy), among others.

Best Practices

- If you need to send unencrypted passwords to a company employee, use alternative communication channels (Telegram, call, SMS).
- Disable the "remember passwords" option in the browser.

Suggestions

- It is challenging to create a strong and easy-to-remember password, especially for multiple services. A good option is to use password management services. With these, you can register a master password, and all others are protected by strong encryption. These managers also offer the option to randomly generate strong passwords. Examples include LastPass, Keeper, BitWarden.

Recognizing a Weak Password:

1. Contains fewer than 10 characters.
2. Is a dictionary word.
3. Is a common word (pet's name, family member's name, movie name, etc.).
4. Includes birthdays or addresses of someone close.
5. Follows common patterns (123456, qwerty, asdfgh, a1b2c3d4, etc.).

Suggestions for Creating Strong Passwords:

1. Substitute letters with numbers or symbols. Example: empresa = 3mpr&s4 / bicicleta = b1c!cl3t@ (A=4, @ / e=3, & / i=1, ! / o=0, etc.).
2. Password length matters! The longer, the more challenging to "crack."
3. Think of a phrase and select the first letter of each word. It's easy to remember and hard to crack. Example:

- My name is John, I live in Colorado since 1780 > MniJiliCs1780
- Apply substitution: MniJiliCs1780> Mn1J!l1Cs!780
- Add a special character:

MniJiliCs1780 > Mn1J1l1Cs1780 > **Mn1J1l1Cs1780#!**

This is a strong password and challenging to crack through traditional means.

Removable Media (USB, External Hard Drive, Smartphone, etc.)

Currently, removable media is a significant concern as storage capacities are increasing every day. While this can be beneficial, it also poses a considerable risk.

External media (USB drives, external hard drives, CDs, DVDs, Blu-ray discs, media cards, among others) enables users to bypass some defense mechanisms, including firewalls and antivirus software. Similarly, a virus from such media can enter the computer without being detected.

Mandatory

- Disable automatic execution for all external media.
- Scan external media with antivirus software before use.
- Never plug in external media of unknown ownership/origin into your device.
- If any of your work equipment malfunctions or requires maintenance, hand it over to the <COMPANY NAME> administrative staff to be sent for technical assistance or properly disposed of.
- Never take your equipment to third parties for maintenance without the company's consent.

Best Practices

- Encrypt important, confidential, or sensitive information/files before copying them to media.
- To minimize any risk (theft, data loss, equipment failure, etc.), store all external media in a secure location.
- Store important information/files on an external hard drive.
- Remove unnecessary content from the device.
- Enable the "show hidden files and folders" option in the operating system.

How to do this on Windows 10:

1. Open File Explorer from the taskbar.
2. Select View > Options > Change folder and search options.
3. Select the View tab, and under Advanced settings, select Show hidden files, folders, and drives, then click OK.

How to do this on Mac:

1. Use the keyboard shortcut "Command (⌘) + Shift + (period)" within Finder.
2. Finder will display the system's hidden folders and files.

Email

Here are the rules and recommendations for the secure use of corporate email:

Mandatory

- Do not save email passwords in browsers.
- Use only the <COMPANY NAME> corporate email address for work-related matters.
- Do not open suspicious attachments or links.
- Do not open emails from unknown sources.
- Do not open attachments with these extensions: Some examples (EXE, DLL, VBS, SHS, PIF, SCR, SH, PY, PL, C).

- **Again: do not open, reply to, or forward suspicious emails.**

Best Practices

- Avoid using the company email on public networks (cafeterias, restaurants, LANs, airports, etc.).
- "Log out" of your email account when you finish work.
- Avoid clicking on links, even if they are from trusted sources. The safest way is to type the URL directly into the browser.
- Be cautious of shortened URLs; do not click if you have doubts about their reliability.

Search for the website on Google “have i been pwned”;

Check your emails;

This website shows if your email has been part of a leak or attack on any site where you've registered throughout your life.

Example: A site you registered on 5 years ago to play a card game was hacked, and all logins and passwords were leaked. The same password you used on that site is the password for another service you use (email, social network, etc.).

Result: your email/social network is vulnerable. You should change that password immediately.

That's why we shouldn't use the same password for various services.

Home Office

With the pandemic, remote work has become the standard model of work. Consequently, potential security risks have emerged. Here are policies related to the topics of remote work and Wi-Fi network:

Mandatory

- Rename your Wi-Fi network (also known as SSID). Choose a name that doesn't reveal any information about you.
- Change the default password of your router.
- Enable WPA2 or another higher encryption for Wi-Fi networks.
- Use <COMPANY NAME> equipment exclusively for work; do not use it for leisure or personal matters.
- Use bags/backpacks when transporting <COMPANY NAME> equipment; do not leave equipment exposed. Never leave equipment unattended in unprotected areas, such as parked cars on the street or valet parking, co-working spaces or cafes, common areas in condominiums, dormitories or lodgings, etc.

Best Practices

- An optional configuration is to filter the use of your Wi-Fi network by MAC (Media Access Control). Every device that connects to your network has a unique physical address, allowing you to add only your devices to your router's configuration. This may be a bit cumbersome if you have many devices or if family members want to connect to your network, but it is an option that complicates unauthorized access.
- Turn off your router when not in use for extended periods. For example, during travel or similar situations.
- Keep smartphones/laptops updated.
- During remote work, keep personal devices on the same network always updated and equipped with quality antivirus software.

- Consider implementing the best practices outlined in this document on personal devices as well. As we currently work from home, there is a risk of transmitting viruses or similar issues to company equipment.
- Use <COMPANY NAME> equipment in a secure and well-ventilated environment, away from children and pets.

Social media

Best Practices

- Avoid using social media or personal accounts on company-owned devices.
- Similarly, refrain from using company email or accounts on personal devices.

Social engineering

Social engineering refers to any form of manipulation conducted in person or socially to obtain personal or business information. It can be carried out through phone calls, emails, or face-to-face interactions. Here are the rules and recommendations regarding this matter:

Mandatory

- Confirm the identity of the recipient requesting information.
- Verify the URL of the website you are visiting. There are sites that closely resemble legitimate ones and are designed to extract information from unsuspecting individuals.
- Delete/block emails or phone numbers that are unknown or suspicious.
- Immediately change passwords that you may have disclosed to someone or that have been part of a data leak.

Best Practices

- Be cautious of calls, emails, and messages from unknown sources.
- Phishing is a common type of attack where information is convincingly requested, often through email. For example, someone posing as your superior (using a similar email that often goes unnoticed) asking for information, passwords, bank account details, and more. Be vigilant! This is very common.
- Vishing is the same as phishing but conducted by voice, i.e., over the phone. Avoid providing information over the phone.
- Scam involves a criminal posing as technical support or something similar to gain access to your machine.
- The safer option is to type the website address instead of clicking on links. Even hovering the mouse over the link and seeing the possible site at the bottom of the screen does not guarantee it's the actual site, as this can be altered by the "attacker."
- If the message/phone call seems urgent, stop and consider whether it is genuinely confirmed. Many cases of manipulation occur through this method.