CMSGu2016-06

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Cyber Security Guidelines for Employers and Employees

CERT-MU

National Computer Board
Mauritius

Version 1.0

December 2016

Issue No. 6

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to raise security awareness and provide corporate employers and employees with essential security information that emphasises critical issues surrounding an implementation of security "best practices" throughout their organisations.

1.2 Audience

The target audience for this document include all employers and employees who make use of computers and the internet at their place of work.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on cyber security issues at work.

Section 3 explains how to empower employees to recognize common cyber threats.

Section 4 provides a cyber security checklist for employees.

Section 5 provides a security checklist for employers.

Section 6 illustrates a guide on cyber security policy for employees.

Section 7 concludes the document.

Section 8 contains a list of references that have been used in this document.

2.0 Background

Everyday new information security threats emerge, and companies find it a challenge to fight these threats. There are various reasons behind these threats, for example, the use of pirated software and not updating your antivirus software. Furthermore, there are employees who download content from untrusted sites, thereby also clicking on malicious links or pop-ups.

Information Security's weakest link is people. Information security is a distributed responsibility and is very important to the survival of any business. Each one of us must make it our personal business to know and adhere to company security policies otherwise security attacks will always present an unacceptable risk to the enterprise and its future well-being.

It is important to note that the risk of an information security breach increases significantly in the following scenarios:

1. Your organisation is involved in a highly competitive business climate
2. Your organisation has terminated an employee that holds a grudge
3. Your organisation has individuals that lack security awareness and best practices

The following sections will guide you through how you can personally prevent a potential information security breach from taking place in your organisation through personal awareness and information security best practices.

3.0 Empowering Employees To Recognize Common Cyber Threats

Empowering your employees to recognize common cyber threats can be beneficial to your organisation's computer security. Security awareness training teaches employees to understand vulnerabilities and threats to business operations. Your employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

New hire training and regularly scheduled refresher training courses should be established in order to instil the data security culture of your organisation. Employee training should include, but not be limited to the following:

3.1 Responsibility for Company Data

Continually emphasize the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

3.2 Document Management and Notification Procedures

Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

3.3 Passwords

Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to employees to change their passwords.

3.4 Unauthorized Software

Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

3.5 Internet Use

Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

3.6 Email

Responsible email usage is the best defense for preventing data theft. Employees should be aware of scams and not respond to email they do not recognize. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.

3.7 Social Engineering and Phishing

Train your employees to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

3.8 Social Media Policy

Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

3.9 Mobile Devices

Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

3.10 Protecting Computer Resources

Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.

3.11 Advising your employees. Talk to Your Employees About

- **Keeping a clean machine**

  Your company should have clear rules for what employees can install and keep on their work computers. Make sure they understand and abide by these rules. Unknown outside programs can open security vulnerabilities in your network.

- **Following good password practices**

  A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, “I love country music.”). On many sites, you can even use spaces! Additionally, having separate passwords for every account helps to thwart cybercriminals. At a minimum, they should separate work and personal accounts and make sure that critical accounts have the strongest passwords. Finally, writing down passwords and keeping them in a safe place away from the computer and enabling two-step authentication are other important ways to secure accounts.

- **When in doubt, throw it out**

  Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source. Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email.

- **Backing up their work**

  Whether you set your employees' computers to back up automatically or ask that they do it themselves, employees should be instructed on their role in protecting their work.

- **Staying watchful and speaking up**

  Your employees should be encouraged to keep an eye out and say something if they notice strange happenings on their computer.

3.12 Training Your Employees

Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe. They also need a basic grounding in other risks and how to make good judgments online.

Most importantly, they need to know the policies and practices you expect them to follow in the workplace regarding Internet safety.

4.0 Security Checklist For Employees

4.1 Social Engineering

1. Be careful that your desire to be helpful in performing everyday tasks does not lead to giving away confidential details to the wrong person about your organisations business.
2. Don’t fall into the trap of trusting a person until they prove to be untrustworthy.
3. Be suspicious if you get a request from someone asking you to fax or email information to them right away, but refuses to provide you a direct callback number.
4. Don’t be intimidated into giving out information to an irate caller, or one who seems to know the structure of your organisation.
5. Watch out for the "odd" request or when a caller asks for information that seems a bit out of the ordinary.
6. Be careful not to cut corners by writing down passwords or leaving confidential material lying around. Securely store confidential material.
7. If you are throwing confidential material away, shred it first.
8. If you print something or have something faxed to you that is sensitive, pick it up right away and store it securely

4.2 Sharing Information

1. Verify positive identity of requestor before providing any confidential information.
2. Verify requestors need to know.
3. Never disclose Level – 4 Restricted Information such as your password to anyone for any reason.
4. Always be aware of how sensitive the information is that you are working with.

4.3 Electronic storage and transfer of information

1. Determine your data sensitivity.
2. Always take a “default deny” stance in providing access to information.
3. Assign security permissions to a role or group rather than to an individual.
4. Only provide the minimum level of access necessary to meet specific business requirements.
5. Remove or disable all unused access IDs and privileges on a regular basis.

6. Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.
7. Classify data you own according to your organisations Information Sensitivity Model.
8. Keep classified data partitioned by as many levels of technology separation as practically possible.
9. Encrypt the transmission of Level–2 Internal and Level–3 Confidential information when sending to an Internet address.
10. Encrypt Level–3 Confidential information when stored in the DMZ or on the Internet.
11. Choose to store important and confidential information on a company network drive.
12. Backup your local hard drive on a regular basis.

4.4 Passwords

1. Do not use family names, nicknames, anniversaries, birthdays, pet names, sports teams or any such items that others would associate you with.
2. Do not use the word “password” for any of your personal password selections.
3. Select a password that is long and strong and a non-dictionary word.
4. Use a minimum of 8 characters using both upper and lower case letters, and a mix of numbers and special characters or symbols.
5. To help you remember your password use the first letter’s of each word in a phrase that means something to you. One way to do this is to create a password based on a song title, affirmation, or other phrase.
6. Never change your password to something known to anyone else, not even for a moment.
7. Keeping your password to yourself is critical to your company’s security. Never share your password with anyone – including your manager, IT Security, IT Help Desk, family, friends or co-workers.
8. Never use the same password for both your work and personal accounts.

4.5 Email

1. Always encrypt sensitive Email and attachments destined to an Internet address.
2. Always delete unrecognized Email. Never open or respond to any Email or attachment unless you positively recognize or trust the sender. This includes spam (junk Email).

4.6 Personal Computers

1. Only install software from trusted sources.
2. Keep all your PC software versions up to date with the most current patches and fixes.
3. Install Antivirus and Firewall software.
4. Never change any settings within your business computer BIOS, the operating system, or any applications (this includes personal firewalls and anti-virus utilities)
5. Never enter unfamiliar commands or run programs at the request of any person unless you can positively verify their identity as a current IT Group employee.
6. Regularly backup critical data on your local hard drives and record your critical configuration settings either to a corporate network drive or a CD-ROM on a routine basis.

4.7 Portable Computers

1. When you leave your portable computer unattended use a security cable to “tie down” your portable computer to a desk or other heavy object.
2. Consider software solutions that will cause stolen portable computers to “call home” when connected to the Internet and GPS devices that will allow you to track your portable computer’s current location.
3. Implement startup security options that will prevent your portable computer from booting into the operating system unless a pass phrase is entered or unless a specific floppy disk is in the drive.
4. Never leave your portable computer unattended, even briefly, in any public place.
5. If you leave your computer in your car, make sure to always keep your car locked and store your computer out of site under a rear pull-cover or in the trunk.
6. Avoid using any storage / carry cases that include a manufacturer’s label on the outside and scream I have a computer inside.
7. On the computer case and the portable computer itself use tamper-resistant tags or directly grave identifying information like your company and personal name and contact information.
8. Never store associated security devices in the same location as your computer. For example, Secure ID Key-Fob / Tokens should never be stored near your desk or in your carry bag next to your computer. Always keep your security devices with you personally or store them in a secure location separate from your computer.

4.8 Telephone Voicemail

1. Do not set your voicemail password to the same number as your phone extension or any other common personal information others might think you could use.
2. It's best to change your voicemail password often, at least every three months, especially if you think you may receive sensitive messages.
3. Follow the Password best practices listed above.

4.9 Wireless Computing

1. Always check with your IT Help Desk to make sure you understand your organisations current policy and procedure before connecting your business computer to another network.
2. Never connect a personal access point, router or bridge to your organisations network.
3. Change your home Access Point / Router / NIC default configurations
    a) Enable encryption and use a key of at least 128 bits.
    b) Change your default access point SSID name to something unique making sure that the new name does not identify who, what or where you are.
    c) Disable SSID broadcasting.
    d) Change the access point's administrator password
    e) Make sure your administrator password is at least 8 characters long and includes a mix of upper and lower case letters and non-alphabetic characters.
    f) If you enable DHCP, limit the number of DHCP Users to the number of wireless computers you will be using.
    g) For Authentication type select "Shared Key" rather than "Open System".
    h) If your access point has an SNMP feature, disable it.
    i) If your access point allows you to select between using a "Short Preamble" or "Long Preamble", select "Short Preamble". A long preamble could make it easier for an intruder to gain entry into your network.
    j) Disable Remote Management.
    k) Disable Remote Upgrade.
    l) Check the access point manufacturer's web site at least once a month for firmware updates and apply accordingly.
    m) Installation of a personal firewall and anti-virus software should be used on all wireless enabled computers.

5.0 Security Checklist For Employers

5.1 Get management approval

To empower employees to face cyber security issues, the management should be first taken into confidence. Without them, the initiative will not be very successful.

5.2 Employ a qualified trainer

It's a good idea for companies to employ a qualified trainer who will give comprehensive training on the subject to the company's employees (as part of their cyber security training initiative). However, this shouldn't be a one-time initiative. It's ideal to regularly conduct cyber security training in the timeframe of six months to one year. The trainer will be able to give information on the latest trends of virus attacks, and discuss case studies.

5.3 Create awareness

In most organizations, as part of cyber security training, the information security division should send out newsletters once a month or once every two months to all company employees. These newsletters increase employee awareness about the latest in cyber security, talk about the latest virus trends, and talk about attack forms.

5.4 Explain responsibility

Generally, during the induction program itself, companies specify the dos and don'ts of the company in the form of a policy. It should be made clear to all the employees that they are responsible for their actions so that in case of a malware attack an employee cannot say that he wasn't aware of the possibility of an attack. As part of their cyber security training, employees should be completely discouraged from downloading software from unknown sites. This doesn't mean they should stop surfing the Internet. What the company can do is add another level of perimeter security wherein the system administrator can regularly audit the system log or the firewall log and find out if somebody is trying to get malicious code inside the company.

5.5 Test the participants

After the cyber security training is over, employees should appear for a test. Based on their scores you can judge their levels of awareness.

5.6 Form an emergency response (ER) team

As part of cyber security training, form an emergency response team. Train the team members intensively so that they are capable of handling all kinds of emergencies.

6.0 Guide To Your Employee Cyber Security Policy

When addressing cyber security threats, human error is a factor that is often overlooked. The first step in reducing the role of human error in cyber security incidents is to establish a cyber security policy for your employees that states the do's and don'ts of cyber security. To help you get started, here is a list of ten points to include in your policy:

6.1 Ten points to include in your policy

1. **Emphasize the Importance of Cyber Security**

   Start off by explaining why cyber security is important and what the potential risks are. If customer or employee data is lost or stolen, this could badly affect individuals involved, as well as severely jeopardize the company. If the company systems are infected with malware, this could severely hamper the efficiency of the company.

2. **Teach Effective Password Management**

   Passwords can make or break a company's cyber security system. Include guidelines on password requirements (for instance a combination of lower case and upper case letters and numbers), how to store passwords (no post-its on your monitor!), how to share passwords (share in person or use the phone instead of email), and how often to update passwords. Also, warn employees not to use the same passwords on different sites.

3. **Detect Phishing and Other Scams**

   Describe the different kinds of phishing emails and scams employees can be presented with and how to spot something 'fishy'. If employees receive an email that looks out of the ordinary, even if it looks like an internal email sent by another employee, they must check with the sender first before opening attachments. When in doubt, go to the company website instead of clicking on a link in an email. Scams can also be perpetrated over the phone, so warn employees about people calling and asking for confidential company information.

4. **Apply Updates and Patches**

   Inform employees to update anti-malware programs, web browsers and other programs regularly and do full malware scans at least once a week.

5. **Protect Sensitive Information**

   Attackers are often after confidential data, such as credit card data, customer names, email addresses, and social security numbers. When sending this information outside of the organisation, it is important that employees understand they cannot just send the information through email. A secure file transfer system must be used that encrypts the information and only allows the authorized recipient to access it.

6. **Lock Computers and Devices**

   When employees leave their desks, they must lock their screens or log out to prevent any unauthorized access. Laptops must also be physically locked when not in use.

7. **Secure Portable Media**

   When using portable devices such as mobile phones and laptops, passwords must be set to limit access. When bringing in portable media such as USB drives and DVDs, it is important to scan these for malware when connecting to the network.

8. **Report Lost or Stolen Devices**

   Advise employees that stolen devices can be an entry point for attackers to gain access to confidential data and that employees must immediately report lost or stolen devices. Often the IT department can remotely wipe devices so early discovery can make all the difference.

9. **Take Active Role**

   Explain that employees must use common sense and take an active role in security. If they see suspicious activity, they must report it to their IT administrator. If employees become aware of an error, even after it has happened, reporting it to IT means something can still be done to minimize the damage. Cyber security is a matter that concerns everyone in the company, and each employee needs to take an active role in contributing to the company's security.

10. **Apply Privacy Settings**

    Inform employees that it is highly recommended to apply maximum privacy settings on their social media accounts such as Facebook, Twitter and Google+. Ask them to make sure that only their contacts can see their personal information such as birth date, location, etc. By limiting the amount of personal information that is available

online, the vulnerability to spear phishing attacks as well as identity theft can be reduced.

The cyber security policy should be included as part of the employment agreement, and regular cyber security training should be scheduled to make sure that employees understand the guidelines. A fun way to make sure that employees understand the policy is to have a quiz that will 'test' their actions in example situations.

In addition to informing and training employees, companies need to ensure that a system is in place for monitoring and managing computers & devices, anti-malware multi-scanning is used to ensure safety of servers, email attachments, web traffic & portable media, and employees can transfer confidential files securely.

7.0 Conclusion

People are considered as the weakest link in the Information Security chain. Information security is a shared responsibility and is crucial to the survival of any business. Every employer and employee must be aware of and comply with enforced company security policies or else cyberattacks will always present an unacceptable risk to their organization and its sustainability.

8.0 References

- **https://staysafeonline.org**
- **https://www.opswat.com**
- **https://www.travelers.com**
- **https://blog.malwarebytes.com**
- **http://www.computerweekly.com**