Safer remote working: Ten basic cyber security practices for Inclusive Finance during CoVid-19, and beyond...

Introduction

The CoVid-19 pandemic has led **many people suddenly to work from home, for many for the first time, and for an unknown duration**. While remote working enables business continuity, an appropriate level of cyber security may not be available in infrastructures, processes, policies, and employees' preparedness to face **more and more frequent and severe cyber risks**.

The financial sector globally is one of the main targets for hackers. Hackers are often organized in international criminal networks; they have advanced skills and tools and are **looking for cash**. Financial inclusion institutions and their large agent networks and emerging digital services have weaker defences than larger institutions. **Employees and agents** using company or personal devices (PC, Tablet, and Smartphone) from scattered locations to access the Core Banking System, or for Digital Financial Services management and other critical business applications, are **excellent channels for intrusion**.

The **recent surge in attacks with many COVID-related scams all over the world** ([1]) should not mask the fact that financial inclusion has to face a **long lasting cyber security challenge** with the proliferation of many techniques that can be mixed: phishing attacks, malicious documents, fraudulent websites, impersonation of government and international organizations' identities, Ransomware, social engineering, fake selling of masks, fake charity donations... While some incidents may be limited to employees' data or finances, many can **endanger the institutions themselves and customer protection: financial losses, data breaches, business discontinuity, reputation damages.**

Employees' outstanding behavior will be the first line of defence. This document aims to share the basic cyber security practices that are easy and cheap to implement and should be **consistently enforced for all your devices.**

1. Regular backup

- **Weekly backup** your documents to protect you against the loss or theft of your device, as well as from corruption or encryption by a malware.
- Backup should include **all your professional documents** including emails, contacts, pictures
- Backup on company servers, online backup service, USB Hard Disk, or USB memory stick.
- Disconnect mobile backup media after use and store it separately from the device, in a safe place.

2. Strengthen your passwords

- **Change default passwords** ("0000", "admin", "1234", "password" for all your devices, including mobile phones' PIN
- Use **long and complex passwords**, preferably the recommended secure passwords. Paraphrases are easily memorized alternatives. For example, "It is time to go to work, John" will become "Iit2gtw,J".
- **Never communicate your passwords** to anybody, either by phone, email, a form on a website, or on a Post It on your screen.

[1] +667% in a few weeks, source Barracuda Networks, March 26th, 2020

- **Regularly change** your passwords
- Use two factors or biometric authentication whenever possible
- ✓ **TIP** Free Password management software will help you with this critical task.

3. Use genuine software, updated to the latest available version

- **Check the installed version** for each device (laptop, tablet, smart phone). If a recent version is not available for your device, as is often the case for older Android smart phones, stop using this device for professional purposes.
- **Use genuine software**: Illegally copied software is often downloaded from compromised websites. Download the software only from reputable editors' official websites.
- **Update systematically to latest version**. Updates containing security fixes should be immediately installed. Check that "automatic update" is selected in your system configuration.
- ✓ **TIP** There are reliable and comprehensive **Open Source** equivalents for most software, including office suite (e.g. LibreOffice).

4. Avoid phishing attacks

- **Phishing emails** contain **links to compromised websites or malicious documents** that will activate malwares if you click or open them, and eventually steal your credentials. These emails usually have the following characteristics:
  - **Impersonification**: the email looks like it has been sent by a trusted party (a bank, a network operator, government services, charities, express forwarder), both in the sender email address and the design of the mail (company logos, text).
  - **Sense of urgency:** to urge you to activate the content ("you have received a prize or a donation", "Your account is about to be suspended", "special sales", "check your bank account data", "urgent invoice", "emergency - send money to"...).
- **Upon reception of an email from an unusual sender or suspect content,** do not open the attached document or click on the link and **delete the mail** immediately. In case of doubt
  - **Check the sender address**: set the cursor over the sender name and the full address will be displayed (may differ between mail clients). The address maybe one of a real person that has been compromised, or one made for purpose, e.g. @paypalinvoice
  - **Check the content** with your search engine. Scams are often shared among cyber experts. Check the spelling.
  - If the mail appears to be legitimate, do not click on the link but connect through your browser, entering the full address, e.g; www.paypal.com.
- ✓ **TIP** Your IT team can give you **additional support on in checking the validity**, and **what to do in case you inadvertently activated malicious content**.

5. Secure web browsing

- **Steer clear of sites or apps with no established reputation**; they are often compromised (games, gambling, software copies, music or video download, illegal or adult contents).
- Be extremely **vigilant when you use payment & banking applications**, set low credit limits.
- Avoid websites using the non-secured protocols http (http**s** is secured).
- Take care of personal, professional information and digital identity including email addresses.

6. Secure your Wi-Fi access

- Set a **strong password** to replace your Wi-Fi router's default password.
- Activate a **strong protocol (WPA2)** and disable Wi-Fi Protected Setup (WPS).
- Create a **guest account** for guests, children, etc. with limited access rights. Never share your credentials.
- **Disable remote access** to the router.

- When travelling: avoid using public Wi-Fi networks unless your organization provides a VPN (Virtual Private Network) to encrypt communication. Use 3G/4G mobile hot spots instead.

7. Take care of all your devices and data

- **Install an antivirus and enable automatic updates**. An antivirus will not protect you from everything, but it is a decent basis.
- **Never leave a device unattended** at home, at the office, or when you travel.
- Make sure sessions are automatically closed after a few minutes of idleness.
- **Do not use a USB memory stick** to share data. Instead, use an online secured file transfer.
- **Protect your workplace**: make sure no one is surfing over your shoulder. Never use public computers.

✓ **TIP**: there are excellent free antivirus softwares.

8. Strictly separate professional and personal uses

- **Company devices** should be **dedicated to professional activities,** not be used by relatives.
- **Do not install any software other than the ones prescribed by your IT** team**.**
- **Close applications or browsers after use**, in particular access to critical business applications

9. You are not alone

- **Contact your IT team** for support on configuring your devices and network access, for any issue or suspicious activity, or if you made a mistake.
- **Contact Law Enforcement Authorities** in case of an incident.

From the company side

10. Ensure you are implementing quickly the basic cyber hygiene measures for secured working from home

- **Awareness raising** is a key component of security of information systems
- Provide a **point of contact and technical support** for employees (access, backup, antivirus software, authorized software...)
- Setup **VPN remote access**
- Establish **a central file sharing with a cloud service provider**, with an appropriate folder structure, document naming, and access settings
- **Check and limit access rights** for all the employees including the IT Team
- **Apply security patches** to fix known vulnerabilities
- **Monitor systems and networks** closely for abnormal behaviours

About Us:

Suricate Solutions is a **pioneering cyber security company for financial inclusion** based in Luxembourg and Senegal where it manages the first cyber Security Operation Centre for financial inclusion. It is the affiliate for Africa for one of the major players in Europe.

As hackers nowadays have virtually access to any system, Suricate has a special focus on operational security, which is the ability to **detect, remediate and recover from cyber security incidents**, and thus drives cyber resilience. A number of services are tailored for financial inclusion, e.g. **security supervision, vulnerability scanning, penetration testing, awareness campaigns, audits, advisory and a "cyber security flash diagnosis"** to assess the maturity of the organisation and identify priority actions.

Contact: jlperrier (at) suricatesolutions (dot) com