Security Awareness Training

Please confirm attendance.

https://docs.google.com/forms/d/e/1FAIpQLSeI736EFdcFXhp18o23ANxVL93JIF04P0U9j_Uzd17rK2eAyQ/viewform

Objectives of this training

- To educate Payreto employees the importance of Information Security, its awareness and practice within and out of Payreto's premises.
- To educate Payreto employees of their role in keeping Payreto safe and secure from leading threats.
- Identify leading threats in Information Security and educating employees on how to combat and avoid them.
- Reiterate our obligation to protect data (especially CHD) through the requirements of PCI DSS.
- Reiterate our obligation to protect data as required by Data Privacy laws.
- Guide employees in reporting incidents relating to Information Security.
- Reiterate the strict observance of the company security policy.
- That you would take this policy and use this knowledge on your daily personal lives as well.

Security Awareness

The knowledge and the attitude of employees and the organization possess regarding the protection of the physical and information assets of the company.

Security

We must protect our computers and data in the same way that we secure the doors to our homes.

Safety

We must behave in ways that protect us against risks and threats that come with technology.

Importance of Security to Payreto

- **The internet allows an attacker to attack from anywhere on the planet.**
- **Risk caused by poor security knowledge and practice:**
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself, our clients, and Payreto)
  - Termination
- **www.sans.org identifies top vulnerabilities for cybercrime are:**
  - Web Browsers
  - IM Clients
  - Web Applications
  - Excessive User Rights

Importance of Security to Payreto

Often, it is the **non-malicious, uninformed employee that is the threat to security** than disgruntled workers and corporate spies.

Don’t be the “uninformed” employee!

https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Uninformed employees can do harm by…

- Visiting websites infected with malware
- Responding to phishing e-mails
- Storing their logon information in an unsecured location or format
- Unknowingly giving sensitive information when exposed to social engineering
- Unknowingly use compromised hardware that can launch an attack internally

https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Not so fun facts…

- **One in five workers** (21%) let **family and friends use company laptops and PCs** to access the Internet.
- **More than half** (51%) **connect their own devices** or gadgets to their work PC. A quarter of who do so everyday.
- **One in ten** confessed to **downloading content** at work they should not.
- **Two thirds (62%)** admitted they have a very **limited knowledge** of **IT Security**.

https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Not so fun facts…

- **More than half** (51%) had no idea how to update the anti-virus protection on their company PC.*
- **Five percent** say they have accessed areas of their IT system they should not have.

* Unauthorized Payreto employees do not have privileges to change PC configuration.
https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

Leading Threats

Malware
Phishing
Social Engineering

Malware

Malware, short for **malicious software**, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

- **Ransomware**
- **Viruses**
- **Worms**
- **Trojan Horses / Logic Bombs**
- **Rootkits**
- **Botnets / Zombies**

Malware explained

Preventing Malware Infection

- **Don’t click on popups or banner ads** about your computer’s performance. Scammers insert unwanted software into banner ads that look legitimate, especially ads about your computer’s health. Avoid clicking on these ads if you don’t know the source.
- **Don’t change your browser’s security settings**. You can minimize "drive-by" or bundled downloads if you keep your browser’s default security settings.
- **Install and update security software, and use a firewall**. Set your security software, internet browser, and operating system (like Windows or Mac OS X) to update automatically.
- **Pay attention to your browser’s security warnings**. Many browsers come with built-in security scanners that warn you before you visit an infected webpage or download a malicious file.

Note that certain actions can only be done by authorized IT personnel.

Preventing Malware Infection

- **Get well-known software directly from the source**. Sites that offer lots of different browsers, PDF readers, and other popular software for free are more likely to include malware.
- **Read each screen when installing new software**. If you don't recognize a program, or are prompted to install additional "bundled" software, decline the additional program or exit the installation process.

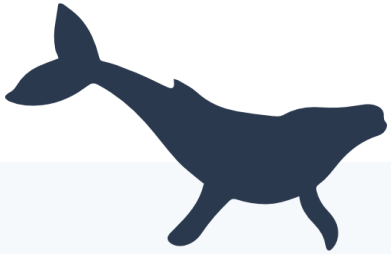
Phishing

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

Types of Phishing

Spear Phishing

A highly targeted form of phishing that hones in on a specific group of individuals or organization.



Whaling

A form of phishing, targeted at executive level individuals.

Cloning

Whereby a legitimate email is duplicated but, the content is replaced with malicious links or attachments.

Anatomy of a Phishing Email

- Contains suspicious links or attachments
- Poor grammar and spelling
- Requests personal or sensitive information
- High sense of urgency and/or privacy
- Discusses confidential subjects like salaries
- Incentives through threat or reward

From: “Bank of America” customerservice@bankofamercan.com
To: “Jane Smith” jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Bank of America

Dear Custumer,

At BOA, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us make Bank of America the safeist bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

* Note that recent attempts where made to Payreto using Dr. Chan’s name and soliciting a wire transfer for EUR 38K received by Simona and Jhevin.

Out-smarting a Phishing Attempt

- Never respond to unsolicited emails that ask for personal information.
- Be suspicious of emails that don't address you by name, have misspellings, or don't look professional.
- Hover over links to verify a link's actual destination, even if the link comes from a trusted source.
- Secure the web address of the site you are logging into rather than clicking on an email link.
- NEVER click on links within unsolicited emails.
- NEVER take on an attacker without the assistance of your security team.
- When in doubt, ask assistance from your security team to verify the legitimacy of an email or verify actions required with the misused identity.

Social Engineering

Social Engineering **manipulates people** into **performing actions divulging** confidential **information**. Similar to a confidence trick or simple fraud. The term applies to the use of **deception to gain information, commit fraud, or access computer systems**.

Social Engineering

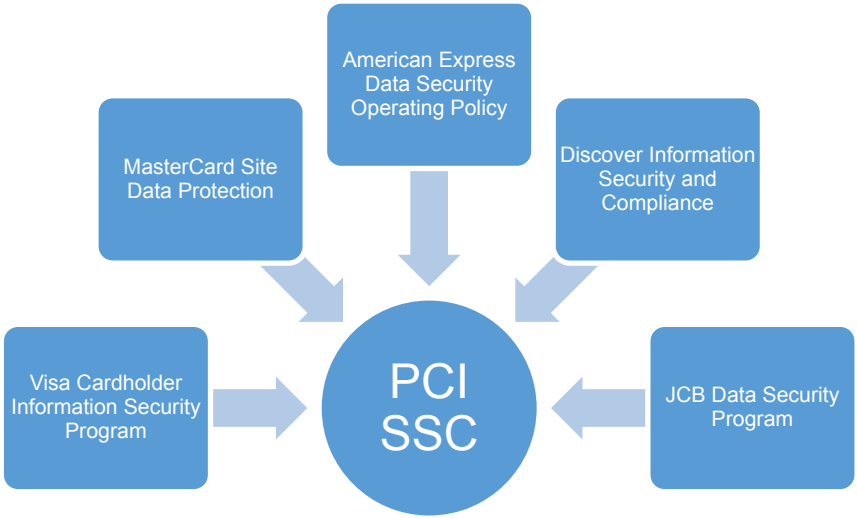
Defenses against Social Engineering

- Educate yourself by taking this Security Awareness Training seriously.
- Be aware of the information you're releasing.
- Determine which of your assets are most valuable to criminals.
- Follow policies and back it up by practicing it.
- Own the security practices of your organization. Be responsible.
- Consider whether the person you are talking to deserves the information they're asking about.
- Watch for questions that don't fit the pretext.
- Challenge suspicious activities. Activate your "fraud sense."

PCI DSS

Payment Card Industry – Data Security Standard

What is PCI DSS?



PCI Security Standards Council ™

- Founded 2014
- Currently on version 3.2
- Unified security standards of different card schemes

PCI DSS is aimed to…

Safeguard cardholders' personal information and facilitate a consistent global data security measure while being stored and/or in transit.

Payment Applications and Devices
(Hardware and Software)

Organization

Network

PCI DSS and Payreto

Payreto's PCI Level 1 compliance is an integral part of our security wide effort that imposes strict adherence of every employee to the company's Security Policy.

Manila	Cologne	Sofia
Level 1	Level 1	Level 1
QSA	QSA	QSA
evolution	Adsigo	Adsigo

Data Privacy

Data Privacy

Data privacy, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

- Healthcare records
- Criminal justice investigations and proceedings
- Biological traits, such as genetic material
- Residence and geographic records
- Ethnicity
- Location-based service and location
- Etc.

Our commitment to Data Privacy

Because of the multinational nature of Payreto as a company, we must abide with the data privacy laws of countries, states, and regions which we operate and do business with.

- Data Protection Directive (officially Directive 95/46/EC) European Union directive
- German Bundesdatenschutzgesetz (BDSG), a Federal Data Protection Act, regularizes together with the Data Protection Acts of the German federal states
- Philippines Republic Act 10173 (Data Privacy Act of 2012) and 10175 (Cybercrime Prevention Act of 2012)
- Etc.

Incident Reporting

What is considered as a Security Incident?

Unauthorized use of hardware or systems.	Unauthorized Access to devices, files or restricted areas	Denial of Service Attack	Malicious Code	Impersonation / Phishing / Social Engineering
Network Systems failure (Widespread)	Application Systems failure (Widespread)	Information Breach	Card Holder Data Breach	Lost / Stolen devices, data repository
Others that directly affect the CIA of data available within Payreto	Incidents that may affect a providers system originating from Payreto			

Incident Reporting Process

All security incidents will initially be reported to IT Security (it@payreto.com) by filling out the Information Security Incident Response

IT Security will report the incident to the entire Security Team (security@payreto.com)

The Security Team, along with other staff, will investigate the incident and assist the compromised department.

The Security Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties.

The Security Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Download the Information Security Incident Response Form

Incident Response

- **DO NOT** attempt to resolve any Information Security Incident on your own. Always involve the Security Team.

- **DO NOT** release information to unauthorized personnel about the nature, status, or execution of plans related to the incident.

- Precisely document using the provided form the nature of the incident and actions done.

Payreto FLEXIBLE WORKFLOW SOURCING

Payreto Security Policy Excerpts

File Sharing and Copyright

- **We respect intellectual property**. Distribution of protected materials are discouraged within our premises and network.
- **P2P programs and torrent applications** are strictly **not allowed** on company PCs.
- Running P2P programs will affect our resources (i.e. bandwidth) and will affect productivity. Thus running such programs is considered as an offense.
- **File sharing sites are breeding ground for malware**. Running and downloading files from these sites may expose Payreto to malware threats.

Facilities Control

- Every employee must be registered for Biometric Authentication (where applicable).
- Every employee must have their own security cards / smart cards (where applicable). No sharing of smartcards.
- **No piggy-backing / tail-gaiting on entry with someone else's access.**
- Only authorized personnel should have physical keys and rights to manually override locks.
- **Badges / IDs must be worn in the premises at all times and visible to other employees.**

Least Privilege and Visitor Control

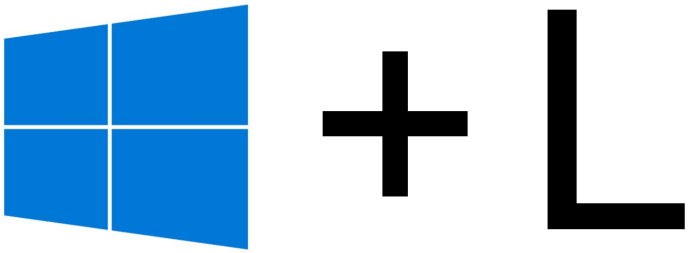
- Every **visitor** must **log in and out** of the Visitor Monitoring Sheet.
- Every visitor must be **issued with a color coded security badge**.

- Depending on the badge, visitors may be **limited on certain areas** only.
- Depending on the badge, visitors **may need to be escorted** in operation / critical areas.
- If not escorted, employees are **required to challenge access privilege** and escort them to the reception area.

Using company computers and devices

- **Only authorized IT** personnel can **change** the **configuration** of a work issued PC.
- Non-authorized employee cannot, without approval, change the physical configuration of the device or use the device other than official business needs.
- **Plugging in of external, non-company owned peripherals** is strictly **NOT ALLOWED.**
- Company issued devices must be registered, tracked, and requires approval from the manager if to be taken out of the office premises or network.
- **Devices of untrusted origin** (e.g. USB drives given on conferences for free) must **not be plugged-in** with any company devices.

Locking your PC



- **Press Windows Key + L Key** to **LOCK** your PC
- Activate **screensaver password lock** that if you forget it your PC will lock automatically.

Working with Card Holder Data (CHD)

- **Downloading**, **storing**, and/or **sending** of **full CHD** are **NOT** allowed.
- To work with CHD for your respective function, it must be **truncated to the barest minimum** before it hits our network (e.g. last 4 digits only).
- IT Security continuously monitor your activity and will alert you and the security team if it detects any CHD or similar data.
- A **high level clearance** and separation (isolation) from the network will be required should a need arise. Strict controls will be implemented.

Paperless Environment

- LOBs with strict policy on paperless or semi paperless environment must abide by the guidelines requested by the client or LOB head.
- Paper based documents that you are not actively working on should be kept in your pedestal.
- Client contracts, invoices, order forms, project scoping and documents in general, containing client information should be stored in a safety box.
- Unused sensitive documents should be shredded according to the standards of the company.

Password Policy

Use STRONG Passwords

- **Use unique passwords for all of your account**
- **Length**

  At least 8 or more
- **Complex**

  Mix upper, lower, numbers, and symbols
- **Do not use common or predictable passwords.**
- **Keep your password secret**

Social Media and Business

- Social media use, at work, should be limited to work-related activities.
- Unless specifically authorized, employees should **not post on behalf of the organization**.
- Employees should **not** share proprietary company information, trade secrets, financial information which may violate policies or protected information about customers, clients, or leads.

File Encryption

- Encrypting a file is like **adding an additional layer of protection** for sensitive files stored or in transit.
- Make it a **habit to encrypt** documents and documents with sensitive information should be **encrypted at all times**.
- Officially we rely on 7Zip for our file encryption. This is a standard application for all employees.
- Microsoft Office documents also comes with password protection and you can protect your documents for storage or for transit.

Call to Action

20%

Technical Implementation

80%

Your Adherence

You owe your clients top notch security.

Payreto FLEXIBLE WORKFLOW SOURCING

Your Security Guidelines Acknowledgement

- [x] Account information is not copied or multiplied.
- [x] Account information is not shared with other employees.
- [x] No information about any Payreto facility, systems or accounts shall be published without authorization.
- [x] No information or data gathered by the use of the provided account is passed to any other person.
- [x] Always lock workstations when leaving the desk.
- [x] Do not use the same passwords for different accounts or systems.
- [x] Use strong passwords (consisting of special characters and numbers).
- [x] Do not attempt to alter your work PCs configuration.
- [x] Make sure every visitor logs in and out of the monitoring sheet.

- ☑ Always wear company issued badges, ID cards within Payreto's premises.
- ☑ Physically lock the door (e.g. keys) when you are the last person to leave the office.
- ☑ Practice clean desk policy and observe a paperless and semi paperless environment.
- ☑ Do NOT connect unregistered BYOD to the Payreto Wireless Network without IT registration.
- ☑ Do NOT store restricted information (e.g. CHD) on your device.
- ☑ CHANGE your password immediately after accessing the BIP on a non-company owned device.
- ☑ All BYOD devices must meet IT requirements prior to registration.
- ☑ Only use company authorized USB devices with your company PCs.
- ☑ No charging of external devices from your company PCs.

Questions?
Feedback?

Don’t forget to acknowledge your attendance (here)
Test your Security Awareness Knowledge (here)

Credits to:

SANS Institute (https://www.sans.org/about/)
ISACA (https://www.isaca.org/pages/default.aspx)
ISO (https://www.iso.org/home.html)

Other Trainings

Coming Soon!

Securing Slack
Securing your files in Google Drive
Using a Password Manager
Detecting a compromised PC
Information Security Incident Reporting
How to encrypt and decrypt sensitive documents
Identifying Phishing Emails
Identity Verification Standards

Thank you!

Don’t forget to acknowledge your attendance here.
Test your Security Awareness Knowledge here.