PROGRAMMED

Information Security & Cyber Security Awareness

What is Information Security

- Information security is what keeps valuable information “free of danger” (protected, safe from harm).
- It is not something you buy, it is something you do.
- It is a process, not a product.

Programmed's Management Systems

Programmed already have a number of ISO certified management systems in place, which has put us in good standing with our customers, suppliers and the general public.

Programmed are seeking certification of our Information Security Management System (ISO27001) in order to meet contractual obligations as more and more of our customers insist we prove our alignment to their security requirements.

ISO International Organization for Standardization

Certified System Quality ISO 9001 SAI GLOBAL

Certified System Environment ISO 14001 SAI GLOBAL

Certified System Information Security ISO 27001 SAI GLOBAL

Certified System ISO 45001 Occupational Health and Safety SAI GLOBAL

bsi. ISO 55001 Asset Management

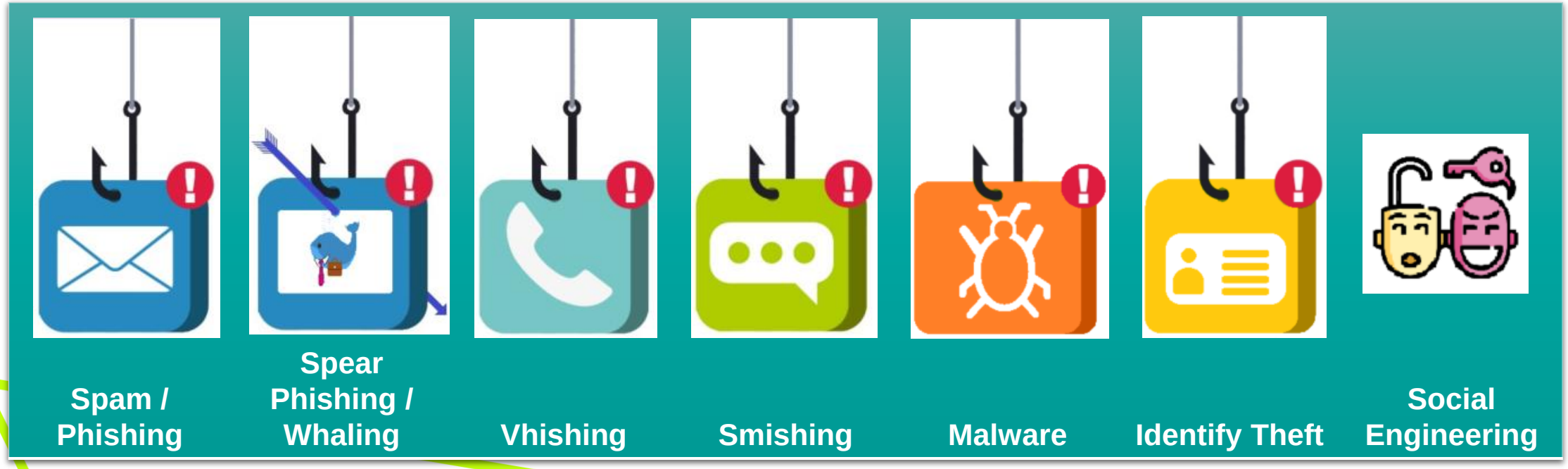
The benefits

Having an Information Security Management System (ISMS) will offer many benefits to Programmed, our clients and our suppliers.

How do we get attacked?

Cyber crimes relate to criminal activity using computer networks and devices to solicit information to illegally obtain money and/or information.

Key areas that affect us all individually are;



Governance

- Everyone needs to be familiar with the Policies, Standards, Processes and Procedures within Programmed and how they impact our daily activities.
- They can all be found within the Intranet…

ISO 27001

- Policies
- Standards
- Processes
- Procedures

Two critical policies

Information Classification Policy

Clear Desk Policy

PROGRAMMED

Information Classification Policy

Establishes the importance of information contained in a document or record and restricts who should be able to see it.

- Applies to all electronic and paper-based information
- Establish 4 levels of Classification;
  - Highly Confidential (Secret)
  - Confidential (Restricted)
  - General (Internal Use Only)
  - Public

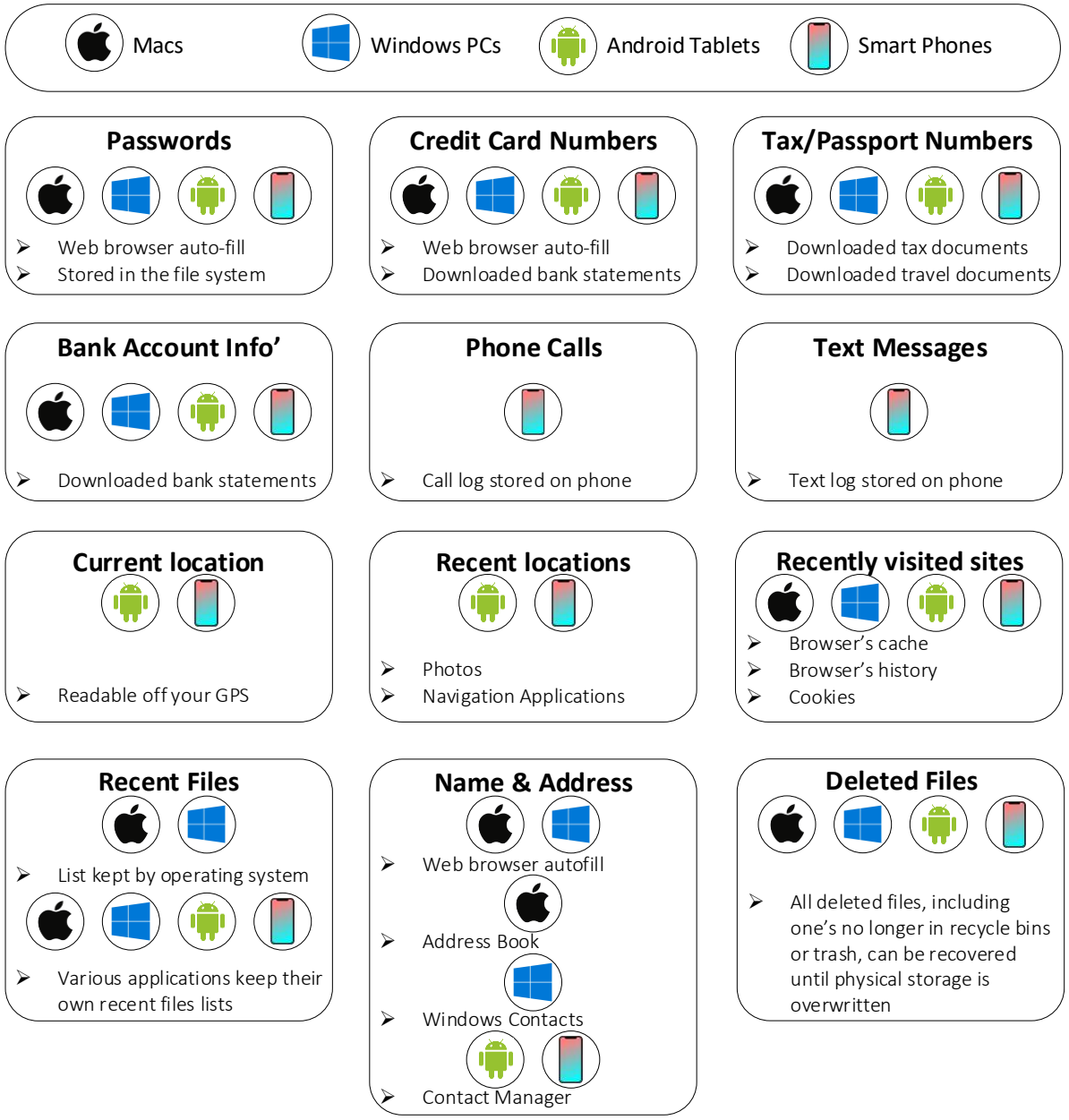
Clear Desk & Screen Policy

To provide protection from unintentional loss through leaving Confidential or Highly Confidential accessible on desks or unprotected devices.

- Locking devices when work areas are unattended.
- Clearing desks of all Confidential and Highly Confidential documentation.
- Locking filing cabinets when unattended.
- Awareness of surroundings and passing observers.
- Clearing presentation materials from whiteboards, flipcharts, etc.
- Disabling screen savers that present an elevated opportunity for malware to be introduced.

Our Devices

- Our dependency on using mobile device for more and more every day activities, means the opportunity for loss of information is ever increasing as portable devices can be easily misplaced or stolen.
- Anyone with malicious intent can learn an awful lot about us by searching through devices for this information and use it for Social Engineering or successful Identity Theft
- What do your devices know about you?



PROGRAMMED

Physical vs Electronic Loss or Theft

- Whilst electronic loss accounts for 84.7% of all data loss, the value of information stored physically should not be underestimated
  - It must be noted, theft or breach in electronic security is significantly easier to detect and has more frequent monitoring and compliance validations performed against it,
  - Whilst loss from a filing cabinet or secure archive facility is often not detected until such a time as the information is required.
- In many instances, the physical loss of information is as a result of poor controls over access to areas where information is stored and through unintentional actions by those who rightfully have access to the information

PROGRAMMED

Thank you