Human Exploits in Cyber security

Authors:
Michael Owino
Ian Koome
Victor Oyuga

Pre-emption

What is Social engineering?

An **attack vector** which **malicious individual(Hackers)** use **psychological manipulation** to exploit **human weakness** to gain **illegitimate access** to information or systems.

Human weakness

Authority

It commands respect to high ranking officials .Commands or emails from high ranking officials are treated with urgency unlike peer staff.

An example is spear –phishing attacks

Liking and Famariality

Use of celebrities by well known companies to push their agenda.

Example is Shoulder surfing, tailgating, Evil twin and pharming.

Human weakness

Reciprocation of favors

Hackers build trust to gain access to information systems.

It takes more time to build trust

Attack vectors – vishing,tailgating,pre-texting(making a situation happen so the victim initiates contact)

Social validation

People are often more willing to do something that others like

Attack vectors – Rogue websites with falsified information, pharming and phishing.

Human weakness

Scarcity

People are often encouraged when they think there is a limited quantity .”Click here to get a free phone”

Attack vector – phishing

Curiosity

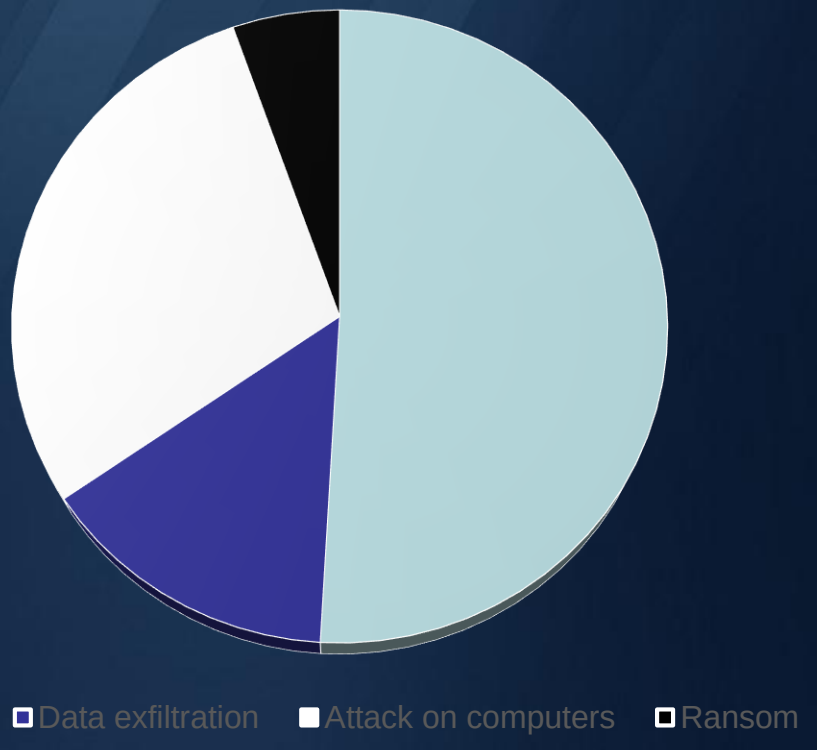
People always want to meddle in other people’s business and this can make them vulnerable.

Attack vector – Phishing, water-hole attacks, evil twin attacks. ”Amazon would like your feedback to the item below …”

Statistics

- Total cost and % of cyber cases in 2017 by Serianu.
- Social engineering attacks

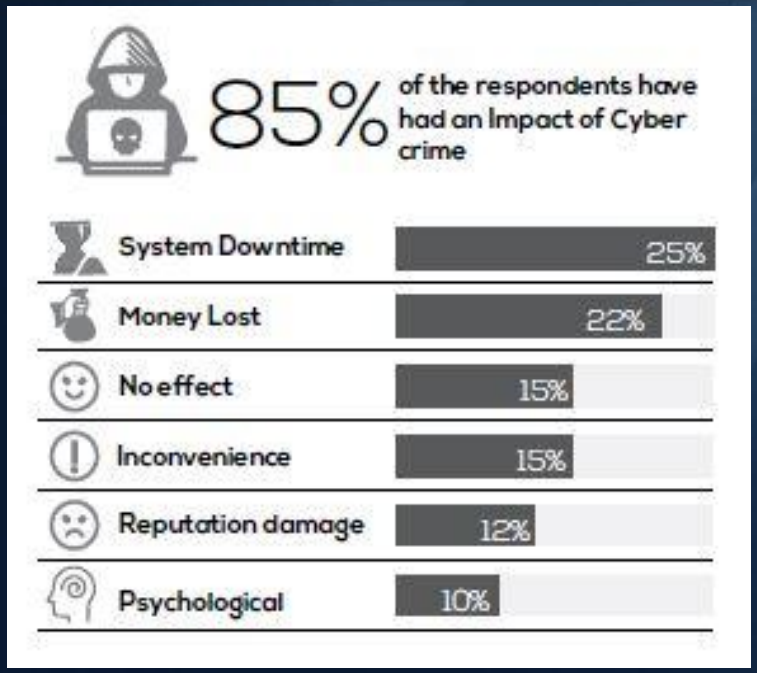
amounted for 65 % of the attacks(worth $136.5) in 2017.



Statistics

Breakdown of attack vectors used in social engineering

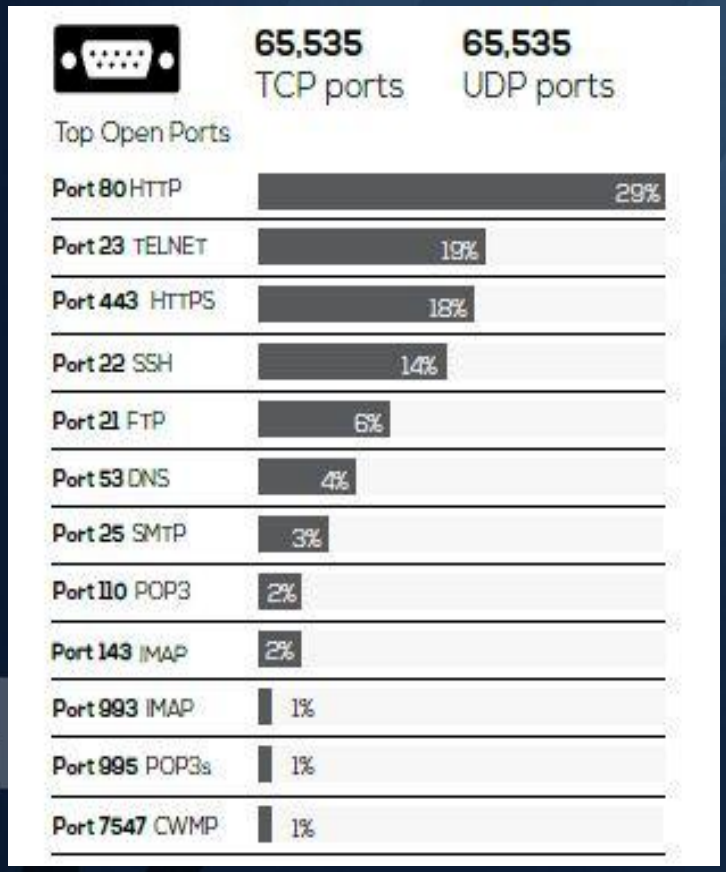
Statistics



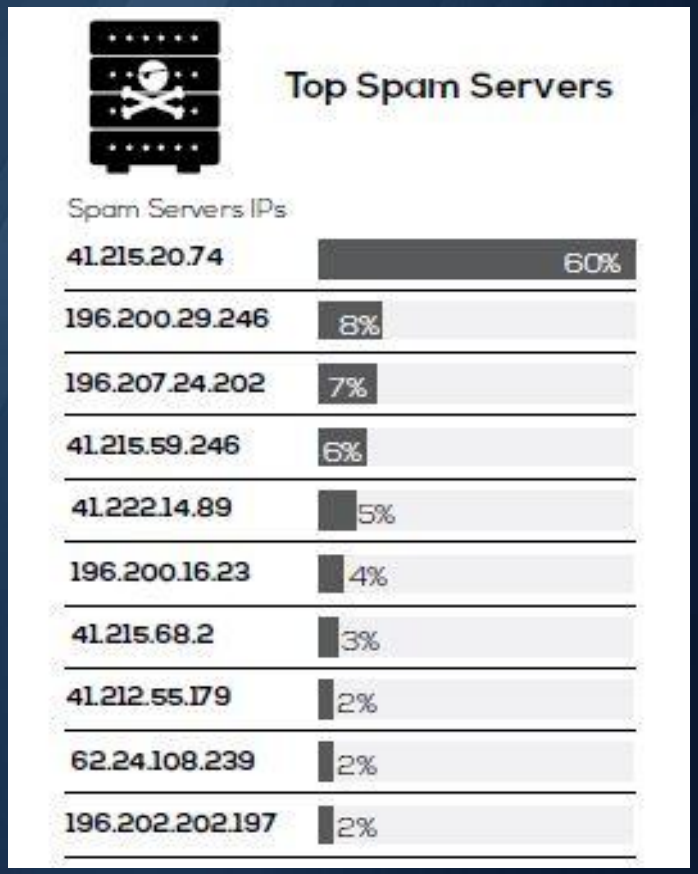
Impacts of social engineering

Most affected Sectors

Statistics



Most attacked ports



Most used spam servers

DEMO

SOLUTIONS

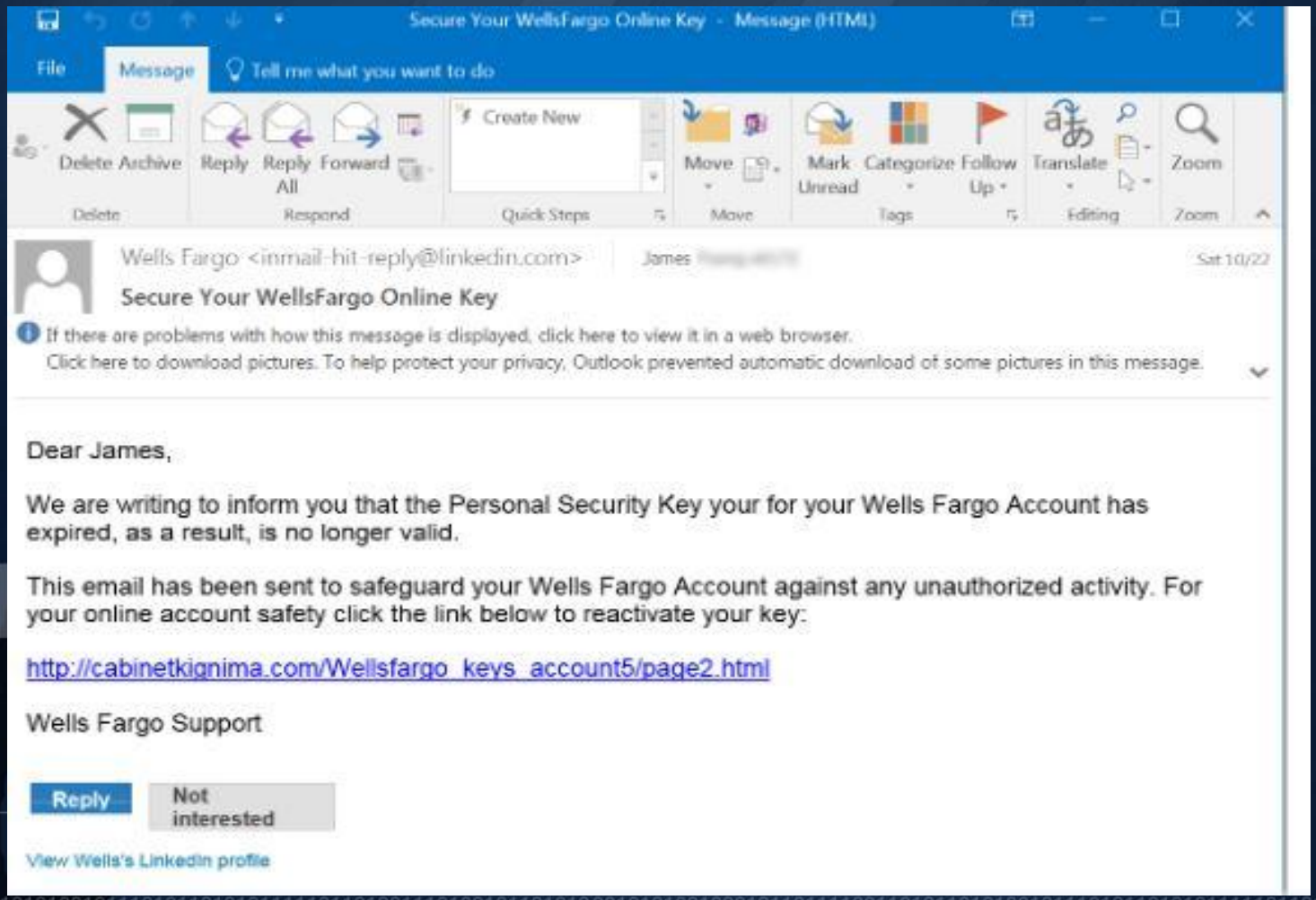
How will we protect ourselves ?

EDUCATE! EDUCATE!

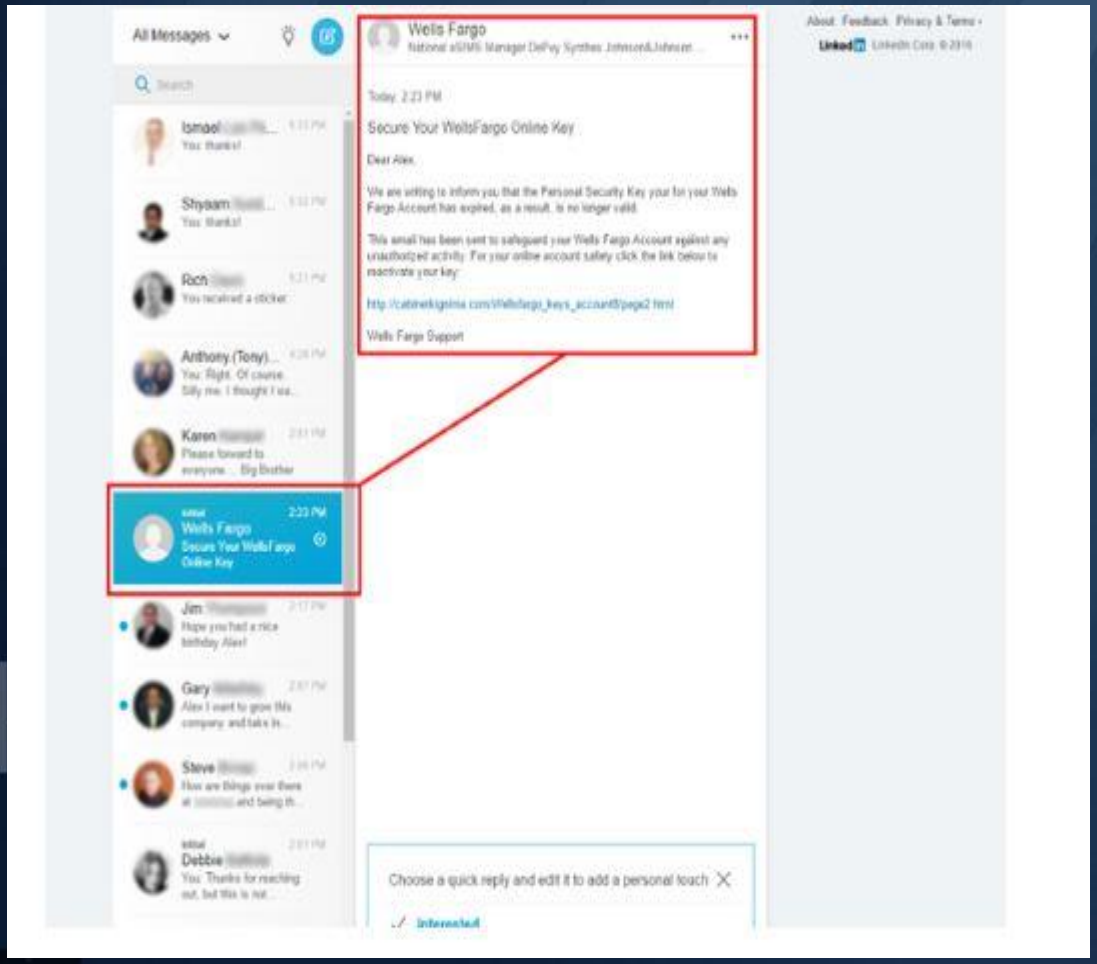
- Use of on-screen keyboards when using highly protected websites for example banking apps
- Scrutinize email before opening the email and attachments too.(Hovering on the links to confirm legitimacy)
- Never share personal information over email / phone ensure proper authentication
- Use ALT +F4 /CMD + Q to close pop ups as you are one clicking away from being infected.
- Never ignore an important update

SOLUTIONS

- How to detect phishing emails

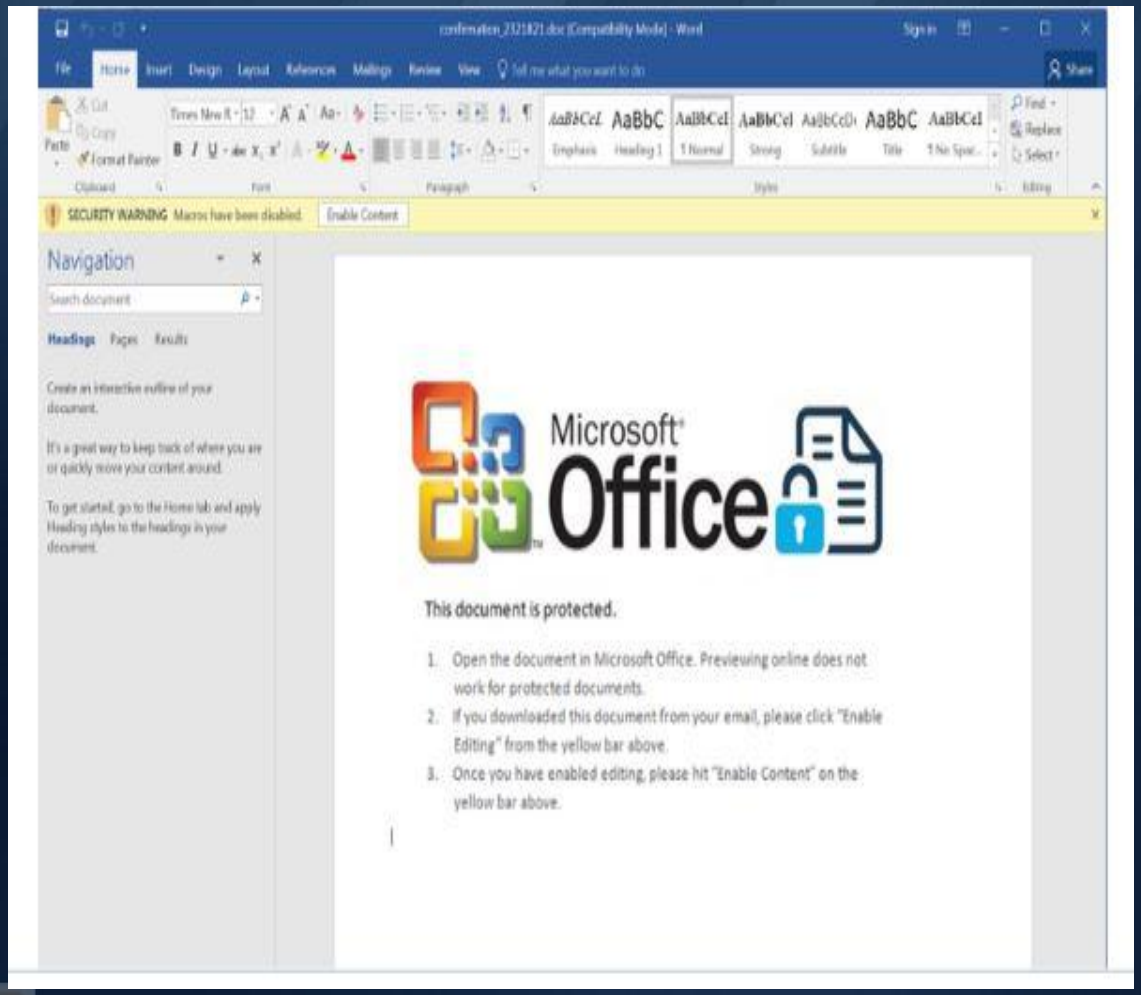


SOLUTIONS



LinkedIn phishing messages

SOLUTIONS



Macros in word documents

SOLUTIONS

- Strict internal policy controls in organizations.
- Frequent assessment of organization security defense.
- Use of sentence – length passwords which are frequently changed.

SOLUTIONS

- Proper employee and contractor management when they resign avoiding insider attacks.
- Defense in depth – use of antivirus , Cisco Stealth watcher(DNS attacks), DMZ, Email proxies.

Remarks

“The internet never forgives and never forgets”