DIGITAL IDENTITY THEFT

DISCLAIMER

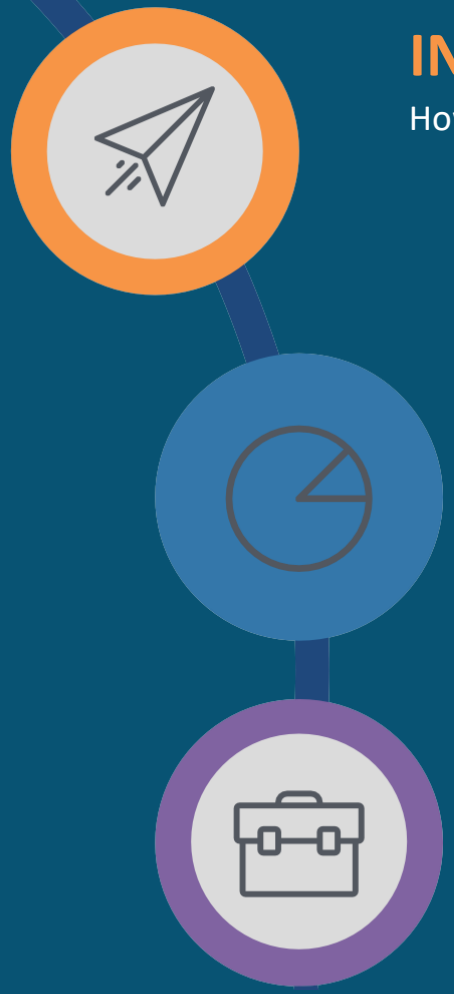
This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

TABLE OF CONTENTS



INTRODUCTION TO DIGITAL IDENTITY THEFT

How and what is the term digital identity describes.

COMPROMISE DIGITAL IDENTITY

Presenting Factors which may compromise a digital identity of a user.

PREVENTING YOUR DIGITAL IDENTITY

Presenting how a digital identity can be prevented by using some basic methods.

INTRODUCTION TO DIGITAL IDENTITY THEFT

INTRODUCTION TO DIGITAL IDENTITY THEFT

A digital identity is a term used to describe a person or an individual who has a unique digital identity which can uniquely identify the user, following are the list of digital identities which are normally used by individuals for identification purpose.

- ✓ Email Address
- ✓ SIM Card
- ✓ Username / User ID (Credentials)
- ✓ Bank Account No
- ✓ CNIC No
- ✓ Passport No
- ✓ Finger Print
- ✓ IP Address
- ✓ MAC Address
- ✓ Host name / Machine Name
- ✓ Digital Certificates
- ✓ Facial Recognition
- ✓ Smart Card
- ✓ RF ID / Token Access

COMPROMISING
DIGITAL IDENTITY

COMPROMISING
DIGITAL IDENTITY

Digital Identity can be compromised if it is not properly secured or overlooked, many people doesn't consider their digital i d to be secure from unwanted users, they provide ID's unintentionally and become the victim of Digital fraud. The below list of digital identities which c an be compromised doing less efforts by the intruder are as follow:

Identity Name	Attack Type	Technique
Email Address	**Email Spoofing**	Forging an email address of a victim and claiming other users that the email is coming from the victim ID.
SIM No	**Caller ID Spoofing**	This technique is used to spoofed a phone number of victim, when a call is landed to the receiver cell phone it seems that the call is coming from a legitimate source.
IP Address	**IP Address Spoofing**	IP Address Spoofing is the technique where an intruder assigned the duplicate IP Address of the Victim, when performing an illegal activity Intruder uses an IP address of the Victim to entrapped him.
MAC Address	**Mac Address Spoofing**	MAC Address Spoofing helps an intruder to impersonate the Victim in order to perform an illegitimate activity over the network, this would help intruder to entrapped a victim.
Hostname / Machine Name	**Hostname / Machine Name Spoofing**	Hostname / Machine Name Spoofing enhances the chances of being untraced over the network, Intruder normally uses a combination of IP Address, MAC Address and a Hostname Spoofing technique in order to completely forged the identity of a person.

COMPROMISING
DIGITAL IDENTITY

Identity Name	Attack Type	Technique
Digital Certificates	**Digital Certificate Forging**	Intruders uses different tools to Signed a forged certificate, if the digital certificate is not pinned with X.509 or a public key, lack of Digital Certificate security allows an intruder conduct a Man in the middle attack and capture sensitive information communicated over the network.
RF ID / Smart Card	**RF ID / Smart Card Cloner**	RD ID / Smart Card Cloner is a device used by the intruders to clone a valid / authentic RF ID Tags / Smart Card of the Victim, normally this attack is use to access the physical or limited access premises within the organization.
Passport No	**Misuse of ID Proof**	Hackers uses Passports for foreign exchange transactions to let their activities goes un-noticed.
Digital Portfolio	**Impersonating Digital Portfolio**	Hacker collect information related to job Seeker's who provide digital CV and personal information regarding Date of Birth, NIC No, Passport No, Address, Fathers Name, Personal Contact No, Personal Email Address. Etc. this information then evaluated by the hackers by identifying the hobbies and interest of an individual in order to exploit them.

PREVENTING YOUR
DIGITAL IDENTITY

PREVENTING YOUR DIGITAL IDENTITY

Preventing digital identity would require the key list of activities which prevent the digital identity from compromising.

1. Email Address Spoofing: Use of special characters in Signature or in conversation made a challenge for the intruders to spoo f the signature of a person, It is highly recommended to use a Line Spacing option while using Signature in an email body;

2. Caller ID Spoofing: The call-back method allows for some security when you think caller ID spoofing is being used;

3. IP Address Spoofing: this attack usually occurred in internal network, controls like VLAN mapping, port mirroring should require to be in place;

4. MAC Address Spoofing: MAC address spoofing usually occurred in internal network, for public network MAC address identity does n't disclose by the system it might disclose by network devices but not by the system. This control requires switch port security, MAC Address whitelisting.

5. Hostname / Machine Name Spoofing: This attack apparently occurred in local network, changing of Hostname must requires admin privileges and it should also be in notice that Hostname Spoofing event ID is 4742 which should generate an alert in SIEM so lution if in case of compromise.

6. Digital Certificates Forging: Forging of digital certificates requires strict pinning of Digital certificate, once the certificate is pinned up it would not be able to bind with the forge one, this can be done under the control panel of digital certificate.

PREVENTING YOUR DIGITAL IDENTITY

Preventing digital identity would require the key list of activities which prevent the digital identity from compromising.

7. RD ID/ Smart Card Cloning: To prevent card-cloning and spoofing, organizations need to make sure they are actually using the features that allow all their cards to be uniquely and securely encoded. Normally encoding factor is missing when developing Smart / RF ID card for the organizations;

8. Passport No: To prevent passport no, do not share the passport information on CV, Internet, Images. It is highly recommended to use passport in an authentic and authorize facility.

9. Impersonating Digital Portfolio: Information Provided in a CV contains (Personal email, Phone No, Date of Birth, Father Name, Passport No) etc. it is highly recommended not to provide detailed information, provide limited information w.r.t. digital identity like name, email, marital status.

THANK YOU