DIGITAL IDENTITY

Version 1.7

Last update on 12/02/2022

by Andrea Nicchi

www.volucer.it

First Draft

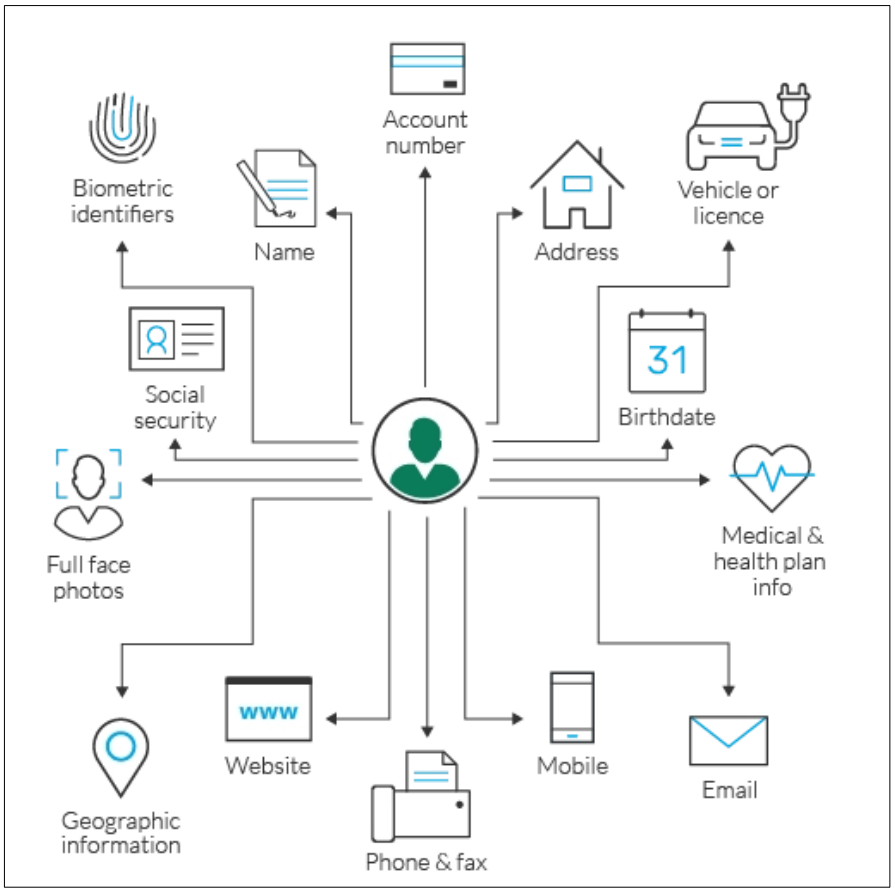
TABLE OF CONTENTS

PII - PERSONAL IDENTIFIABLE INFORMATION

According to the NIST (National Institute of Standards and Techonology, the following items definitely qualify as PII, because they CAN unequivocally identify a human being:

full name (if not common), face, home address, email, ID number, passport number, vehicle plate number, driver's license, fingerprints or handwriting, credit card number, DIGITAL IDENTITY, date of birth, birthplace, genetic information, phone number, login name or screen name.

PII - PERSONAL IDENTIFIABLE INFORMATION



“quasi identifiers” or “pseudo identifiers”:

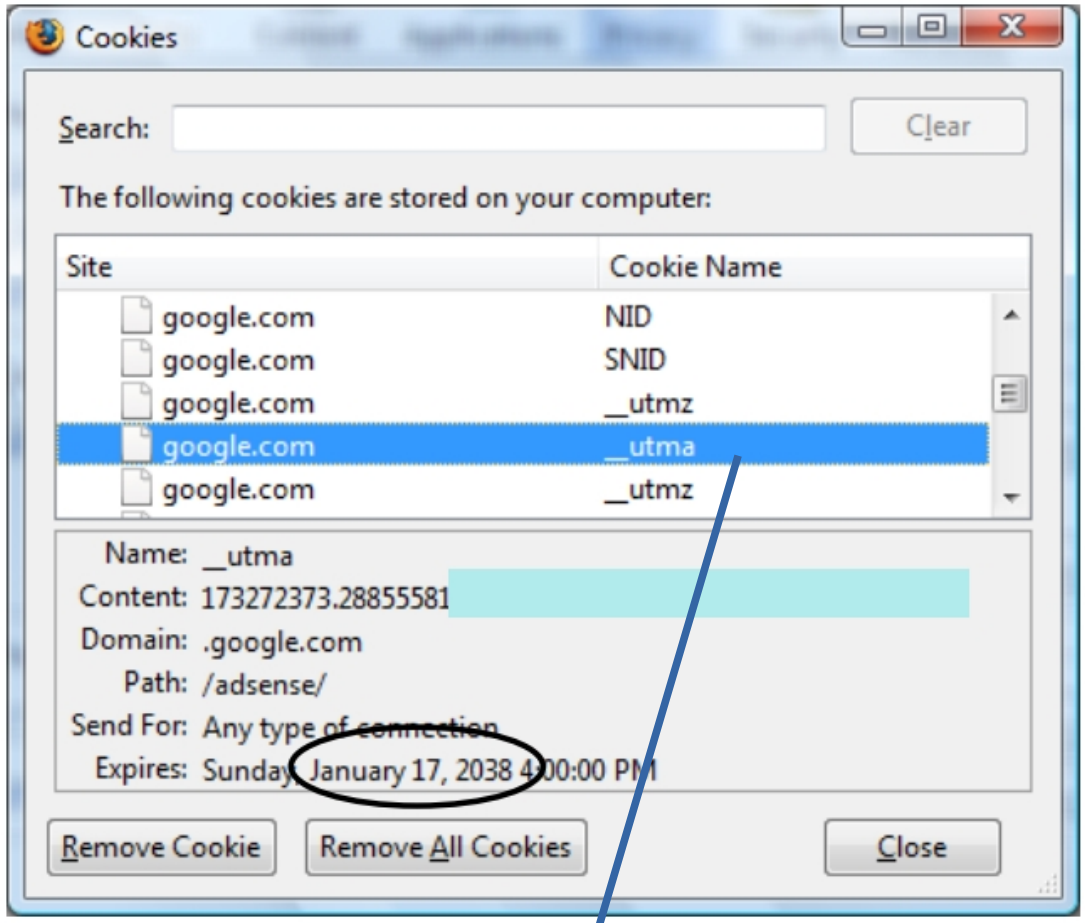
a combination of gender, ZIP code and date of birth

DIGITAL IDENTITY

DIGITAL IDENTITY: is the data that uniquely describes an entity such as people, organizations or things and contains information about the subject's relationships. Any personal data existing online that can be traced back to real you.

For example: photos you have uploaded, post you have created or commented on, your online bank account, search engine history an so on.

DIGITAL IDENTITY



__utma cookie (persistent) lives forever (never expires) and identifies you. This cookie is usually installed in the browser on the first visit. This cookie is used to determine unique visitors to our website and is updated with each page view.

```
__utma=1.32168570.1258672608.1258672608.1259628772.2&__utmb=1.4.10.1259628772&
```

DIGITAL IDENTITY

DIGITAL IDENTITY IS IMPORTANT: it ensures access to on-line services – financial, health-related or educational.

Digital identity management is fundamental for the further development of the Internet Economy (Digital Economy)

It raises the issue of how to translate the mechanisms through which individuals trust each other as a prerequisite to interaction in the digital world. Managing digital identity is essential for the Internet to operate as a platform for economic development and social progress.

OECD - Organization for Economic Co-operation and Development

https://www.oecd.org/sti/ieconomy/digitalidentitymanagementandelectronicauthentication.htm

DIGITAL IDENTITY

TYPES OF DIGITAL IDENTITY

- **government**: for taxation …
- **organizational**: school, corporate, …

- **customer**: bank,
- **user**: nickname, pseudonym, ..some degree of anonymity,

- **transactional**: temporary identity

- **anonymous**:

DIGITAL IDENTITY

TYPES OF DIGITAL IDENTITY

- **networking**: ip address

- **machine:** serial number, MAC (Media Access Control) address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

- **attributes**: a collection of attributes that together identify an entity.

DIGITAL IDENTITY

DIGITAL IDENTITY MANAGEMENT

The digital identity lifecycle generally involves several processes:

1. REGISTRATION / ENROLMENT PROCESS: to be known by the system, the individual must first register with it and the conditions related to his/her identity or identity attributes must be checked so he/she can be provided with a set of credentials.

2. AUTHORIZATION: appropriate permissions and privileges to access the organisation's resources must be assigned to the individual.

DIGITAL IDENTITY

DIGITAL IDENTITY MANAGEMENT

3. **AUTHENTICATION PROCESS**: to access resources, the individual makes an identity claim that can be verified: he/she logs into the system with the credentials provided during the registration process. It establishes confidence in the user's identity.

4. **ACCESS CONTROL**: the system checks that the individual has the appropriate authorization to access the resource.

5. **REVOCATION**: When the individual is not associated anymore with the system, a revocation process must take place whereby his/her credentials are rescinded.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

also called ONLINE REPUTATION is defined as the prestige of a person, is the perception that others have of your.

Therefore, digital reputation management assumes its significant value for business success.

97% of entrepreneurs say that reputation management is the key to success.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

HOW TO TAKE CARE OF OUR DIGITAL REPUTATION

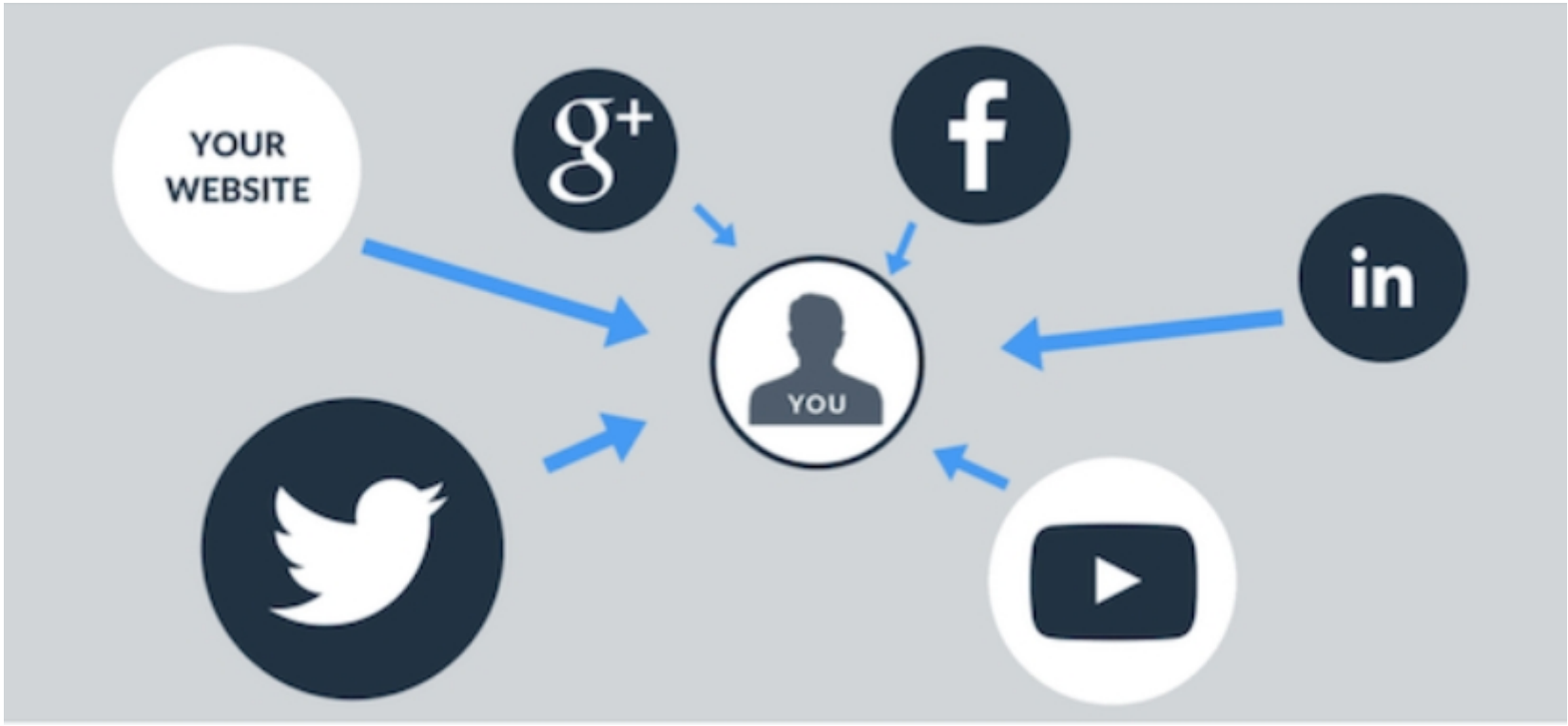
SEARCH ENGINE: in which page you appears, because in our experience and numerous studies, very few people go beyond the first page.

People are looking you up online at every stage of your career & making decisions about you based on what they find.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

HOW TO TAKE CARE OF OUR DIGITAL REPUTATION



Source:https://brandyourself.com/online-reputation-management

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

DIGITAL REPUTATION AND SOCIAL NETWORKS

SOCIAL NETWORKS CAN CONTRIBUTE TO A GOOD REPUTATION

OR ON THE CONTRARY, DESTROY IT.

Twitter: it is important to participate, contribute and establish conversations with other users in the sector. In order to further disseminate your content, you must share original and useful messages.

LinkedIn: is essential to have a suitable photo and have an updated resume. Publish articles and statuses. Comment on the statuses of other users.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

DIGITAL REPUTATION AND SOCIAL NETWORKS

SOCIAL NETWORKS CAN CONTRIBUTE TO A GOOD REPUTATION

OR ON THE CONTRARY, DESTROY IT.

Facebook: you must appropriately manage the privacy of your account. In it he must share publications, constantly, that contribute something to his followers.

Personal web: is to have a personal blog or website that is also well positioned in search engines.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

TOOLS FOR CHECKING ONLINE REPUTATION

https://brandyourself.com/: keep track of where your name is coming up in the search engines.

https://about.me/: allow you to set-up a web page that's all about you. You can direct people from Facebook or Twitter to it to learn more about you.

http://www.socialmention.com/ if you want know about mentions of you.

http://www.whostalkin.com/ mentions and alerts about mentions of you

https://namechk.com/ makes sure noone is using your name on any of the social media.

DIGITAL IDENTITY

PERSONAL DIGITAL REPUTATION

TOOLS FOR CHECKING ONLINE REPUTATION

https://www.google.it/alerts: alerts for any search you want

http://www.yasni.com/ s it very easy to keep track of what people are saying about you online

https://www.spokeo.com/; http://www.pipl.com/; http://www.cvgadget.com/

These ones utilize deep web crawlers to aggregate data. Searches can be made for a name, email, phone number, username or address. These sites allow users to remove information about themselves through an "opt-out" process.

DIGITAL IDENTITY

DIGITAL FRAUD: PSYCHOLOGY

Real attack exploit psycology, victims are lured by email to log on bogus website, it easy for crooks to build a bogus bank website.

ASYMMETRY ONLINE-FACE-TO-FACE FRAUD

On-line frauds is easier to do and harder to stop. It is different from deception in face-to-face contexts.

In the on-line hoaxes and frauds we lose physical and human context that implies high risk to be involved.

DIGITAL IDENTITY

ATTACKS BASED ON PSYCHOLOGY: PRETEXTING

The most common way to steal personal information is pretexting: phoning someone pretending to be someone authorised to be told it. Such attacks are sometime known collectively as Social Engineering.

Kevin Mitnick's "The art of deception" (2002): almost all of his exploits had involved social engineering.

USB Stick as part of anonymous invitation or a gift.

DIGITAL IDENTITY

ATTACKS BASED ON PSYCHOLOGY: PHISHING

It is a harder problem for a company because the targets are not your staff but your customers.

The attacker often reuses genuine bank emails with just the URLs changed. Customers who use the provided link rather then typing it are compromised.

DIGITAL IDENTITY

AUTHENTICATION PROCESS

It is the act of verifying someone's identity. Bob must be sure that he is communicating with Alice and not someone trying to impersonate her. Alice's can use three types of methods:

1. **something you know;**
2. **something you have;**
3. **something you are.**

DIGITAL IDENTITY

AUTHENTICATION PROCESS: SOMETHING YOU KNOW

Bob asks Alice for some secret only she should know, such as a password. Passwords are one of the biggest pratical problems facing security engineers today. Password schemes are simple to implement but:

- most users do not choose strong passwords so they are easy to guess or easy to crack. It occurs to force user to choose passwords that are hard;
- user needs to reuse a password each time he logs into a system – an attacker has numerous opportunities to "listen in". One-Time Password (OTP) eliminates the risk but no user will be able to remember all these passwords;
- ATM PIN bank can freeze the account after three wrong guesses, no limit on the number of guesses for an encrypt document with a password.

DIGITAL IDENTITY

AUTHENTICATION PROCESS: SOMETHING YOU KNOW

WEAK PASSWORD CHOICE – HUMAN FACTOR

Weak passwords are passwords that are easy to guess, or likely to be found in a dictionary attack.

November 2013 - Adobe confirms stolen passwords were encrypted, not hashed

Source code and 2.9 million accounts raided by attackers in Adobe breach] Researchers have revealed, and Adobe has confirmed, that the millions passwords stolen during the breach in October were not originally stored according to industry best practices. Instead of being hashed, the passwords were encrypted, which could make things a little easier for those looking to crack them.

PC WORLD - 123456: Millions of Adobe hack victims used HORRIBLE passwords

DIGITAL IDENTITY

AUTHENTICATION PROCESS: SOMETHING YOU ARE

WEAK PASSWORD CHOICE

N.	Count	Password	Percentage
1	1911938	123456	37.81 %
2	446162	123456789	8.82 %
3	345834	password	6.84 %
4	211659	adobe123	4.19 %
5	201580	12345678	3.99 %
6	130832	qwerty	2.59 %
7	124253	1234567	2.46 %
8	113884	111111	2.25 %
9	83411	photoshop	1.65 %
10	82694	123123	1.64 %
11	76910	1234567890	1.52 %
12	76186	76186	1.51 %
13	70791	abc123	1.40 %
14	61453	1234	1.22 %

They are 3.994.331 of 5056923

and represent the 78.99 % of all stolen password.

DIGITAL IDENTITY

AUTHENTICATION PROCESS: SOMETHING YOU HAVE

OTP CARDS: SecurID Card generate a new password each time a user needs to log in. It flashes a new passwprd to the user periodically e. g. every 60 seconds. The server knows the algorithm that the SecurID uses to generate passwords and can verify the passwords that the user enters.

SMART CARDS: they are tamper-resistent. It means if a bad guy tries to open the card or gain access to the information stored on it, the card will self-destruct.

ATM (Automatic Teller Machine) Cards: they aren't tamper-resistent. Anyone who has magnetic stripe reader can access the information stored on the card.

DIGITAL IDENTITY

AUTHENTICATION PROCESS: SOMETHING YOU ARE

It is based on something that the user is:

- ✔ biometric authentication: palm scan, iris scan, retinal scan or fingerprinting;
- ✔ voice recognition;
- ✔ facial recognition;
- ✔ signature dynamic: parameters: signature, pressure and timing.

Disadvantages:

- ◆ false positives and negatives generated;
- ◆ we cannot revoke the user's key.
- ◆ Inefficient once attackers are able to impersonate biometric measurements.

DIGITAL IDENTITY

AUTHENTICATION PROCESS: MULTI-FACTOR (MFA)

Combining various authentication techniques can be more effective.

The term TWO-FACTOR AUTHENTICATION is used to describe the case in which a user is to be authenticated based upon two methods.

Alice with a cell phone with GPS activated in front a ATM machine is requesting to withdraw money. Bank can ask her cell phone company's computer system where she currently is.

Client Authentication

Server Authentication

Mutual Authentication

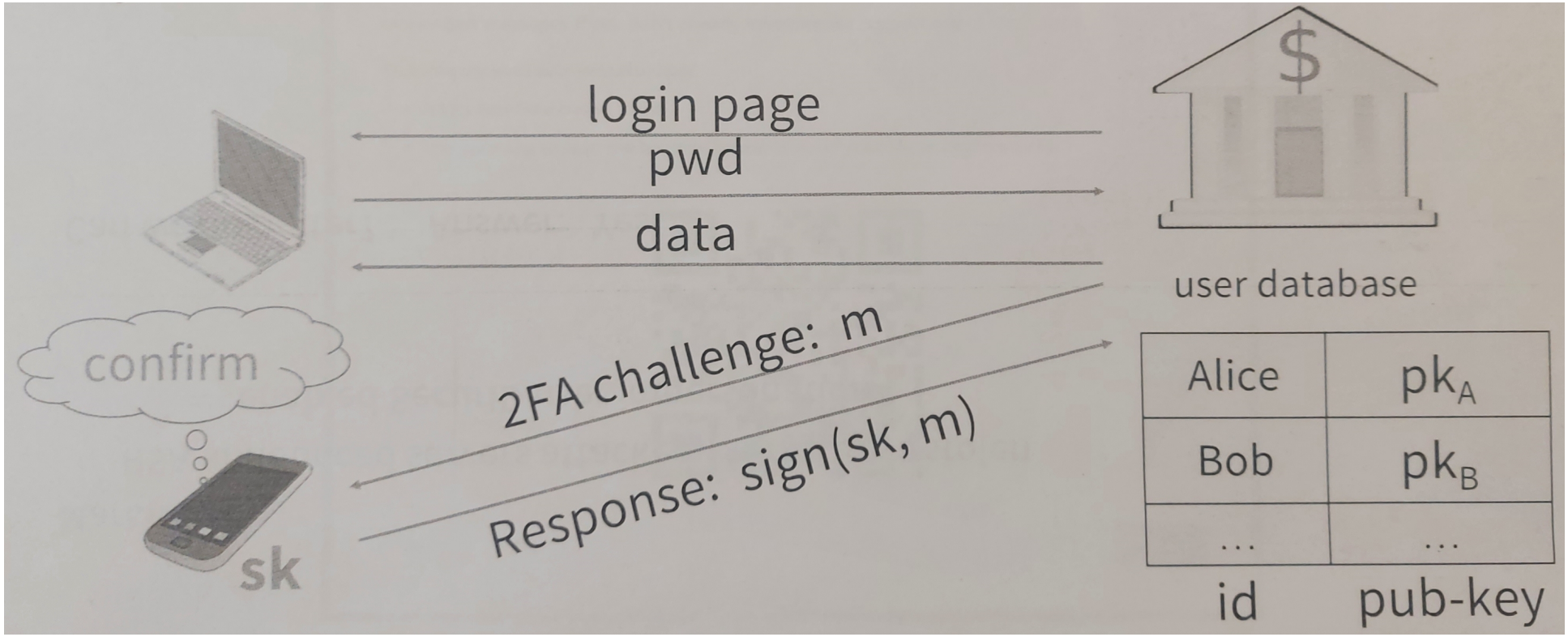
DIGITAL IDENTITY

AUTHENTICATION PROCESS: TWO-FACTOR AUTHENTICATION

DUO, FIDO U2F(Fast Identity online – Universal Second Factor)

SIGNATURE -BASED CHALLENGE RESPONSE:

NO SECRETS ON SERVER; SIMPLE USER EXPERIENCE



DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: INTRODUCTION

ATO is defined as an unauthorized access and control of a legitimate user's account (a user account is an identity created for a person in a computer or computing system).

Unauthorized user may change account credentials and lock out the legitimate user or change notifications methods;

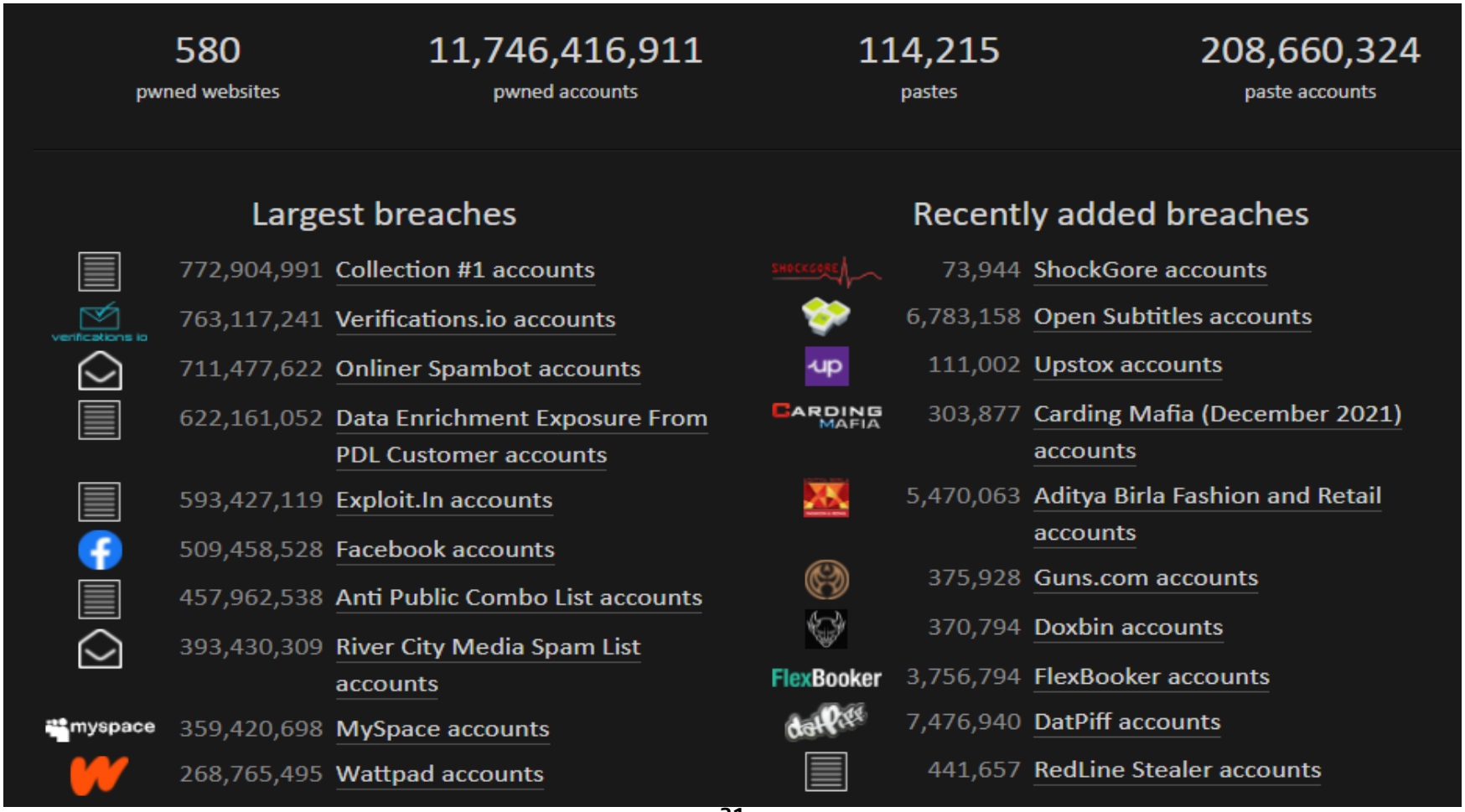
Generally user has several PERSONAL and BUSINESS accounts. Many users continue to use the same passwords on various account.

Once an account is compromised, it provides access to an existing digital identity or the ability to create a fraudulent one.

DIGITAL IDENTITY

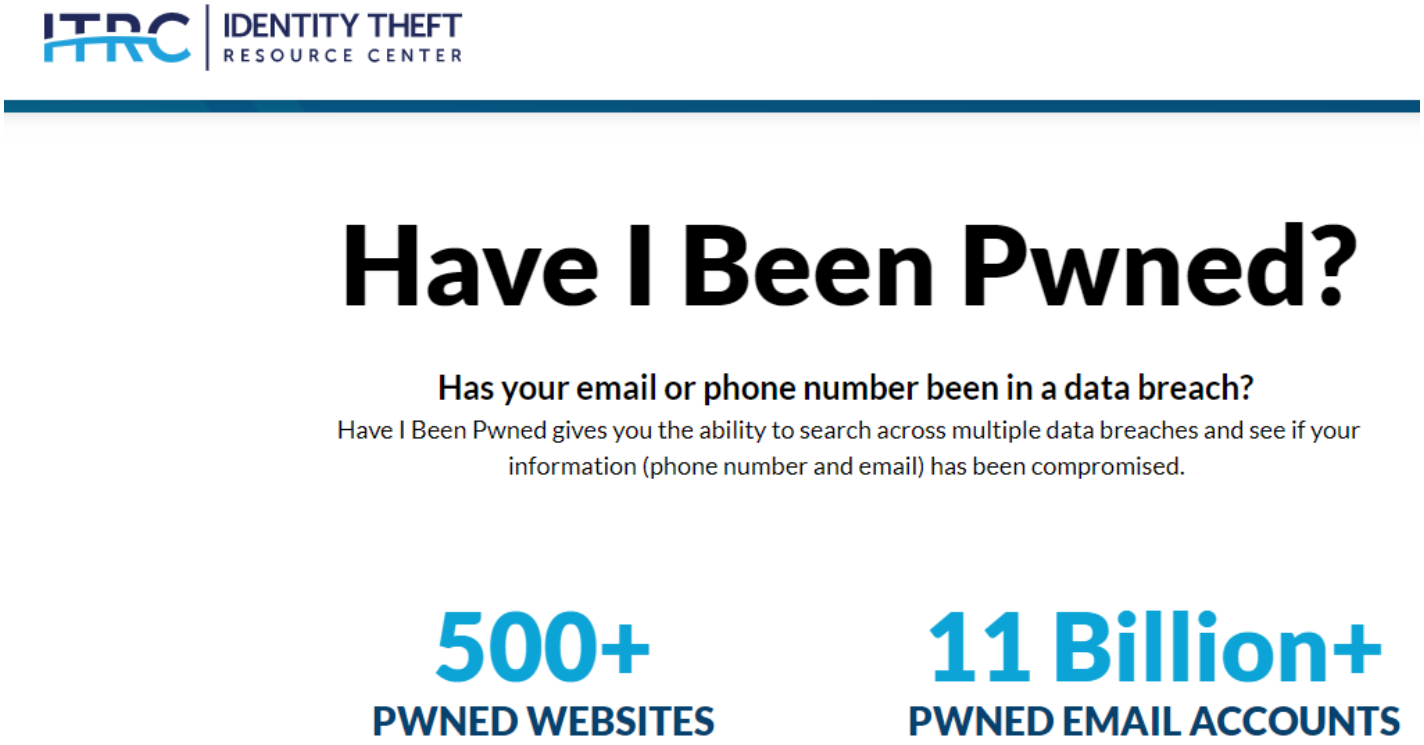
ACCOUNT TAKEOVER (ATO) ATTACK: VOLUME OF LEAKED CREDENTIALS

https://haveibeenpwned.com/



DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: VOLUME OF LEAKED CREDENTIALS



https://www.idtheftcenter.org/ Word Population:7.9 billion people 2021

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: BIGGEST DATA BREACHES

Ranked by Impact (https://www.upguard.com/blog/biggest-data-breaches)

1. CAM4, March 2020, 10.88 billion records
2. Yahoo, October 2017, 3 billion accounts
3. Aadhaar, March 2018, 1.1 billion people
4. First American Financial Corp., May 29019, 885 million users
5. verifications.io, February 2019, 763 million users
6. Linkedin, June 2021, 700 million users
7. Facebook, April 2019, 533 million users
8. Yahoo, 2014, 500 million accounts
9. Marriott, November 2018, 500 millions guests
10. AdultFriendFinder, October 2016, 412.2 million accounts
11. MySpace, June 2013, 360 million accounts
12. Exactis, June 2018, 340 million people
13. Twitter, May 2018, 330 million users

14. Adobe, October 2013, 152 million

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREATS

To obtain legitimate user credentials, adversaries may use myriad of tactics and attack vectors including:

SOCIAL ENGINEERING: consists of tactics used to gain access to PII, systems, data, or money by manipulating human psychology. (phishing, SMSishing or vishing – phone call, angler phishing on social media).

CREDENTIAL STUFFING: using a list of stolen credentials to gain unauthorized access to user account.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREATS

BRUTE-FORCING: submitting and systematically checking many potential passwords in an attempt to crack password codes.

SESSION HIJACKING: accessing unauthorized access to a valid user session in an attempt to exploit information.

EXPLOITING VULNERABILITIES: finding specific web application flaws to gain access to customer databases.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREATS

DETECTION PROBLEM

SUCCESSFUL LOGIN RESULTING FROM AN ATTACK ARE INDISTINGUISHABLE FROM NORMAL USER LOGIN ACTIVITY, MAKING DIFFICULT TO DETECT AND DEFEND AGAINST.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREAT ACTORS

ACTORS POPULATION

While the total number of ATO actors is unknown, the partition of the set is more or less clear:

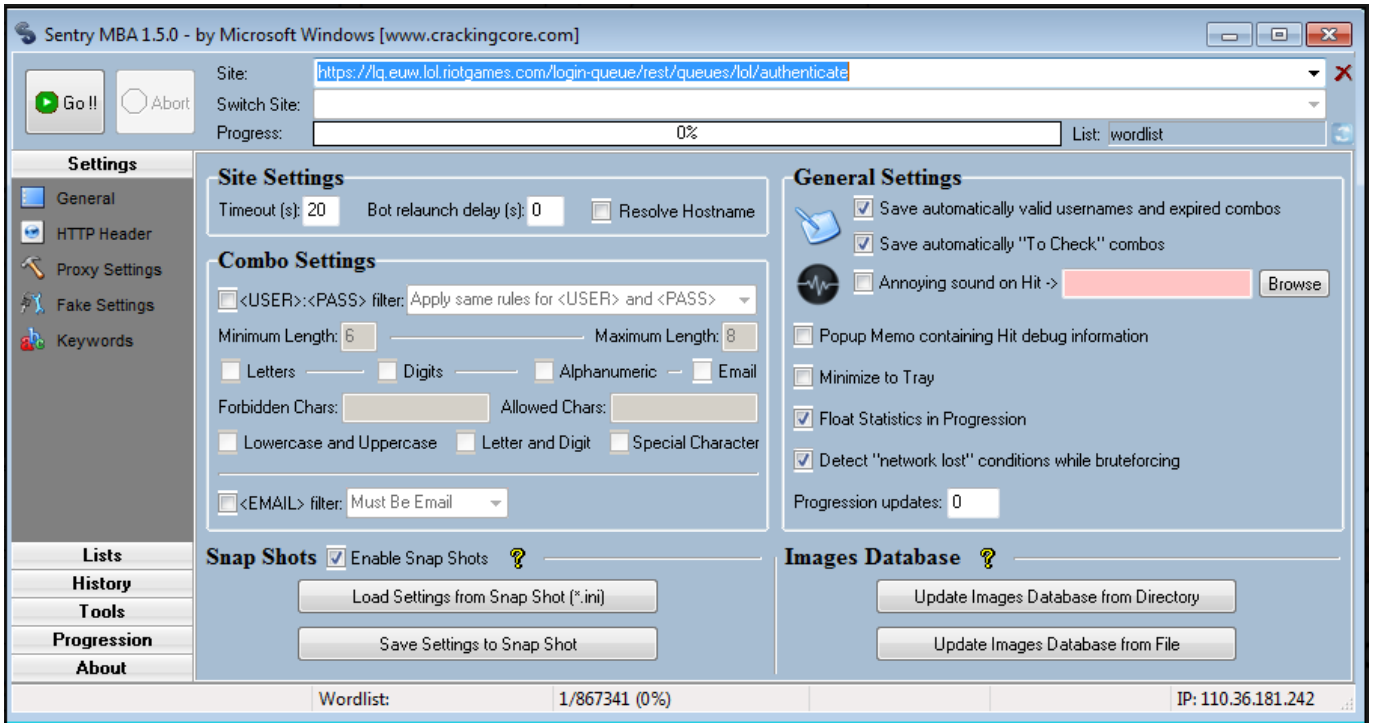
- Majority are opportunistic category: teenagers or young men;
- Sophisticated actors are a small fraction;

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREAT ACTORS

CASUAL OPPORTUNISTIC OR LOW SKILLED ACTORS

One method used by opportunistic actors is brute-force attacks by using a common tool Sentry MBA.



DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREAT ACTORS

CASUAL OPPORTUNISTIC OR LOW SKILLED ACTORS

Sentry MBA

- ✔ It attacks nearly every website that requires a username and password.
- ✔ you can test millions of accounts on your targeted website automatically.
- ✔ It is a very user-friendly and easy-to-use tool.
- ✔ It is used by hackers and crackers to hacks millions of online accounts of different websites like (Netflix, Instagram, Twitter, Amazon Prime etc many more).
- ✔ This tool has so many artificial intelligence base advanced features to auto bypass captcha security.
- ✔ This tool also uses the proxies list in this. It means Ip addresses of different countries.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREAT ACTORS

CASUAL OPPORTUNISTIC OR LOW SKILLED ACTORS

Another method used by opportunistic actors is “account checkers”.

An account checker is an attack tool that takes lists of spilled username/password pairs (i.e. “credentials”) and tests them against a target website.

- ✔ account checkers can be stand-alone or web-based;
- ✔ pay-per-use model: account checker as a service;
- ✔ leverage lists of usernames and passwords;
- ✔ verify if accounts are valid at a specific site or service;

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: THREAT ACTORS

SOPHISTICATED ATO ACTORS

- significantly higher skills;
- develop custom tools and scripts for specific target;
- modify their attacks in response to blocks;
- their activity is much harder to detect;

Methods:

- ✔ simulate legitimate traffic using custom configuration of browser emulation technology;
- ✔ hijacking legitimate accounts for use in fraud or further ATO activity;
- ✔ Malware installed on victim's system allows to capture keystrokes to steal password or capture session credentials and cookies.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: MONETIZATION

CYBERCRIMINALS ECOSYSTEM: DEEP and DARK WEB (DDW) forum and marketplaces represent the primary means by which products and services are bought and sold.

As-a-service offerings for targeted exploition gives even unskilled cybercriminals the opportunity to attack high profile and hardened targets.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK

Between Q2 2020 and Q2 2021, fintech companies have seen an astronomical 850% increase in attempted ATO, primarily concentrated in crypto and digital wallets.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: PREVENTION

ACCOUNT CREATION: once an account has been created, I should validate (authorization code – via mail or mobile phone). User should set up multi-factor authentication.

PASSWORD POLICY: use strong/robust password and change it frequently.

ACCOUNT LOGIN: when a user attempts to login, limit any validated verbiage when an incorrect username or password has been entered: "incorrect password", "email is not associated with an account".

IP BLOCKING: temporary blocking IP that login to multiple accounts simultaneously or accounts that are accessed from multiple IP address. Use geolocation to limit fraudulent activity.

DIGITAL IDENTITY

ACCOUNT TAKEOVER (ATO) ATTACK: PREVENTION

ACCOUNT MONITORING THE LAST DEFENCE

Once users have successfully logged into an account monitoring and management controls provide a gatekeeper function to prevent and detect unauthorized activities that may lead to loss of covered data.

- ✔ **Limit potential exposure of sensitive information;**
- ✔ **musk full payment card numbers;**
- ✔ **require re-entering of full credit card numbers and passwords;**
- ✔ **Use geolocation;**
- ✔ **Automatically lock access or logoff users after 15 minutes of inactivity.**

DIGITAL IDENTITY

EMAIL ACCOUNT TAKEOVER (ATO) ATTACK

WHEN IF YOUR EMAIL ACCOUNT IS COMPROMISED

- ✔ You are unable to access your e-mail account. An attacker gained access to your email address and changed the password to lock you out of the account.
- ✔ Your family, friends, and coworkers receive emails from you that you didn't write. The attacker can use your email address to send spam or phishing emails to the contacts in your address book.
- ✔ You see activity on your social media accounts that you didn't post.
- ✔ You notice your Sent messages folder is empty or includes messages that you did not send.

Source: https://www.cisecurity.org/newsletter/compromised-email-account-heres-what-to-do/

DIGITAL IDENTITY

EMAIL ACCOUNT TAKEOVER (ATO) ATTACK

WHAT TO DO IF YOUR EMAIL ACCOUNT IS COMPROMISED

- ✔ Login to your email account and reset your password using a strong password.
- ✔ End / sign out of all sessions on all devices.Even after you change your password, if the attacker has an active session, they may be able to continue to send emails from your account.
- ✔ Enable Multi-Factor Authentication (MFA) on your e-mail account.
- ✔ Review and change your security questions.
- ✔ Review your mailbox for any rules that you have not previously created.

DIGITAL IDENTITY

EMAIL ACCOUNT TAKEOVER (ATO) ATTACK

WHAT TO DO IF YOUR EMAIL ACCOUNT IS COMPROMISED

- ✔ Review outgoing messages and retract any malicious outgoing messages.
- ✔ Contact the people in your email address book and let them know that your email was compromised. Remind them to delete any emails from you during the time your account was compromised to prevent them from becoming the next victim.
- ✔ Verify if there is private or personally identifiable information in your e-mail that could be used maliciously.
- ✔ Establish a routine where you change your password periodically.
- ✔ Scan your computer for viruses and malware.

DIGITAL IDENTITY

Назарыңызға рахмет!

Спасибо за внимание!

Thank you for your attention!