SOCIAL ENGINEERING

Dr. Ala Berzinji

WHAT IS ‘PERSONAL INFORMATION’?

Information that can be used to distinguish or trace an individual’s **identity**, either alone or when combined with other information that is linked or linkable to a specific individual.

PERSONAL INFORMATION ONLINE

- Create a mind map of all the reasons that people might use the internet
- For each reason, add any risks to personal information
- For each risk, add any ways to stay safe and protect personal information

SOCIAL ENGINEERING

Social engineering is the manipulation of people into carrying out specific actions, or divulging information, that is of use to an attacker.

SOCIAL ENGINEERING

- A hacker might undertake social engineering for information gathering.
- Their motivation might also be personal revenge, to prove a point,
- Or they may hack out of personal enjoyment or boredom.
- Through social engineering, a hacker could do many things with financial gain or account information. For example, they might lock someone out of their accounts, sell their data, take over someone's financial assets, or take a loan out in someone else's name.

SOCIAL ENGINEERING

Email account	• Send a phishing email to contacts
Social media account details	• Impersonate the person for personal gain
Banking details	• Spend money or take out loans
Online business information	• Threaten to release information to the public
Personal data	• Sell the data to companies; identity theft
Access to gaming accounts and videos	• Hold the account to ransom
Online shopping history	• Sell information to companies so they can target their advertising

PRINCIPLES BEHIND SOCIAL ENGINEERING

- Authority
- Intimidation
- Consensus/social proof
- Scarcity
- Urgency
- Familiarity/liking
- Trust

SOCIAL ENGINEERING

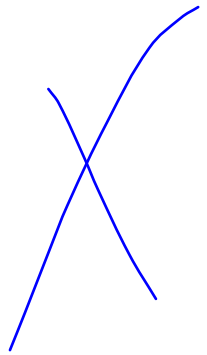
- Hardware locks and security
  - Involves applying physical security modifications to secure the system(s)and prevent them from leaving the facility
- Mantraps
  - Require visual identification, as well as authentication, to gain access

CYBER AWARE

1. Use a strong and different password for *email accounts*
2. Create strong passwords for all accounts
   (e.g. use three random words)
3. Turn on 2-step verification (2SV)
4. Save passwords using a browser or a password manager
5. Back up data
6. Update devices

SOCIAL ENGINEERING

- Biometrics
  - Use some kind of unique biological trait to identify a person, such as fingerprints, patterns on the retina, and handprints
- Alarms



WHAT IS MISINFORMAION?

- **Misinformation:** False or incorrect information
- **Purpose:** Affect the perception of people

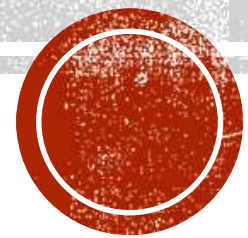
PROBLEM OVERVIEW:

- The large use of Online Social Networking has provided fertile soil for the emergence and fast spread of rumors.
- It is difficult to determine all of the messages or posts on social media are truthful.
- Fake news harms to real life.

CURRENT SOLUTIONS:

- Data Representation
- Deep Syntax
- Semantic Analysis
- Discourse Analysis
- Classifers

PRIVACY AND CYBERSECURITY



WHAT IS PRIVACY

- Privacy has different meanings in different contexts and societies.
- Linked to security and to control of immediate environment - what is known or can be known about us.
- Exact definitions are elusive – national and international courts have refused to provide clear definitions of privacy.
- There can be tensions between freedom of expression rights and privacy rights.

PRIVACY IS NOT DATA PROTECTION

- Data protection rules are designed to address the systematic collection of data about individuals and the rules apply to all personally identifying data held by designated “data controllers”.
- Privacy is more fluid concept applying to information about which a person may have a reasonable expectation of privacy.

MEANING OF PRIVACY CHANGES

- Personal integrity lies at the heart of privacy.
- Privacy in a communal village or modern city very different.
- Also shaped by technology, e.g. modern notions growing from debate about newspaper photographs.
- No exact boundary, a dramatic technological change like the Internet will inevitably re shape understandings of privacy.
- Contrast between what people say about privacy and the internet and how they behave.

THE INTERNET

- Enables the collection of new types of personal information
- Facilitates (and economically demands) the collection and location of personal information
- Creates new capacities for government and private actors to access and analyse personal information
- Creates new opportunities for commercial use of personal data
- Creates new challenges for regulation given the transnational nature of the internet.

INTERNET SERVICES REDEFINE PRIVACY ENVIRONMENT DRAMATICALLY

- Cloud computing (raises questions of security, data breaches and ownership),
- Search engines (systematically track and monitor our behaviour),
- Social networks (depend on a company led exchange and analysis of data provided by users),
- The mobile internet (ties internet use to geo-located devices);
- Internet of things connecting all potential objects which together convey a complete picture of our lives

GOVERNMENT USE OF DATA

- E-government - governments moving to digital platform and provision of services.
- Government increasingly seen as a digital platform.
- Some governments have designated e-identities that allow services, banking, voting, health monitoring etc.
- With the sheer volumes of data available it is difficult to conceive that governments won't seek to access it.
- How to balance the provision of e services (much cheaper than human services) with security and personal privacy.

INTERNET IS BUILT AND OPERATED BY THE PRIVATE SECTOR NOT A PUBLIC UTILITY

- Provision of internet services based on a **business model based on advertising.**
- We trade or cede our privacy in exchange for free services.
- Such service models either directly depend upon exposing private information (Facebook).
- Or intrude on privacy to create efficiencies (tools that optimize searches based on tracking user preferences).
- Generally little real public pressure or incentives to challenge this model.
- Informed consent to data use for users online is complicated by range of different applications, complexity of terms of use, and apparent public indifference.

ECONOMIC GROWTH AND INTERNET

- New emphasis on economic growth and internet development
- Increasing pressures for data sharing, cross border transfers of data
- But a business environment that depends on people feeling secure and that categories of information – financial, health etc. need to have guaranteed confidentiality
- Cybersecurity – understood as providing privacy – is essential to internet based economy

PRIVACY OFFLINE AND ONLINE

- Privacy online should be protected as privacy offline –Need to understand what is new about the environment and how to tackle it.
- All will depend upon strong security both technically – encryption – and normatively – legal rules governing access to and use of personal information.

WHAT IS THE PRIVACY AGENDA?

- personal integrity (basis of data protection system) and what can be known.
- Current business models require us to hand over ownership of our data to companies in exchange for benefits -use of that data is loosely regulated if at all.
- Government access to data.

GOVERNMENTS SHOULD

- Commit to ensuring user security and privacy as a policy goal
- Commit to freedom of expression, aware of the need to balance both rights
- Understand cyber security as embracing users interests
- Be transparent about the rationale and scope of surveillance or other measures violating privacy
- Ensure that rules governing surveillance and privacy violations are grounded in law.
- Consistent with international principles and subject to supervision by independent courts
- Regulate effectively e.g.by having technical skills

COMPANIES SHOULD

- Practice greater transparency about data management practices
- Provide accessible and reasonable terms of service
- Encourage higher standards of encryption and anonymity, as both are enablers of privacy rights
- Publish details about government requests for user data

CIVIL SOCIETY ROLE

- To bring concerns from excluded and marginalized groups
- Provide innovative ideas and policy options
- To champion a public interest approach to privacy policy