

সোশ্যাল ইঞ্জিনিয়ারিং

সোশ্যাল ইঞ্জিনিয়ারিং আক্রমণ হলো, কাউকে প্রতারণা করে কোন তথ্য সংগ্রহ করা। সাধারণত এই কাজটা যাদের সাথে করা হয়। যেমন- রিসেপশনিস্ট, হেল্পডেস্ক সাপোর্ট পারসন ইত্যাদি।

সোশ্যাল ইঞ্জিনিয়ারিং এর ধাপসমূহ-

ধাপ-০১: টার্গেটেড কম্পানি নিয়ে রিসার্চ (ওয়েবসাইট, কর্মীদের তথ্য, ডাম্প পেপার সংগ্রহ)

ধাপ-০২: প্রতারণা/হতাশাগ্রস্ত কর্মীকে খুঁজে বের করা

ধাপ-০৩: প্রতারণা/হতাশাগ্রস্ত কর্মীর সাথে সম্পর্ক তৈরি করা

ধাপ-০৪: প্রতারণা/হতাশাগ্রস্ত কর্মীর কাজ থেকে তথ্য সংগ্রহ করা

কতভাবে সোশ্যাল ইঞ্জিনিয়ারিং করা যায়?

সাধারণত তিনভাবে-

১. হিউম্যান বেসড সোশ্যাল ইঞ্জিনিয়ারিং

২. কম্পিউটার বেসড সোশ্যাল ইঞ্জিনিয়ারিং

৩. মোবাইল বেসড সোশ্যাল ইঞ্জিনিয়ারিং

হিউম্যান বেসড সোশ্যাল ইঞ্জিনিয়ারিং

Human-based Social Engineering: Eavesdropping and Shoulder Surfing



Eavesdropping



- Eavesdropping or **unauthorized listening of conversations** or reading of messages
- Interception of audio, video, or written communication
- It can be done using **communication channels** such as telephone lines, email, instant messaging, etc.

Shoulder Surfing



- Shoulder surfing uses direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done from a longer distance with the aid of **vision enhancing devices** such as binoculars to obtain sensitive information

Computer-based Social Engineering: **Phishing**

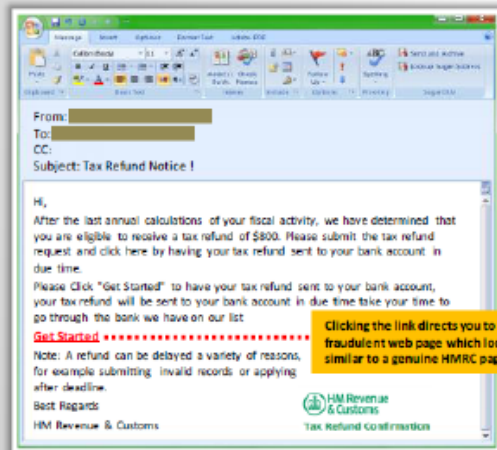
CEH
Certified Ethical Hacker



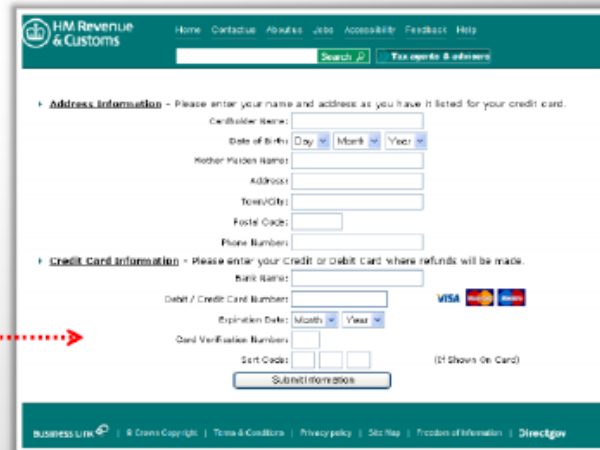
An **illegitimate email** falsely claiming to be from a **legitimate site** attempts to acquire the user's personal or account information



Phishing emails or pop-ups redirect users to **fake webpages** of mimicking trustworthy sites that ask them to submit their personal information



Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page



৩. মোবাইল বেসড সোশ্যাল ইঞ্জিনিয়ারিং

Mobile-based Social Engineering: Publishing Malicious Apps

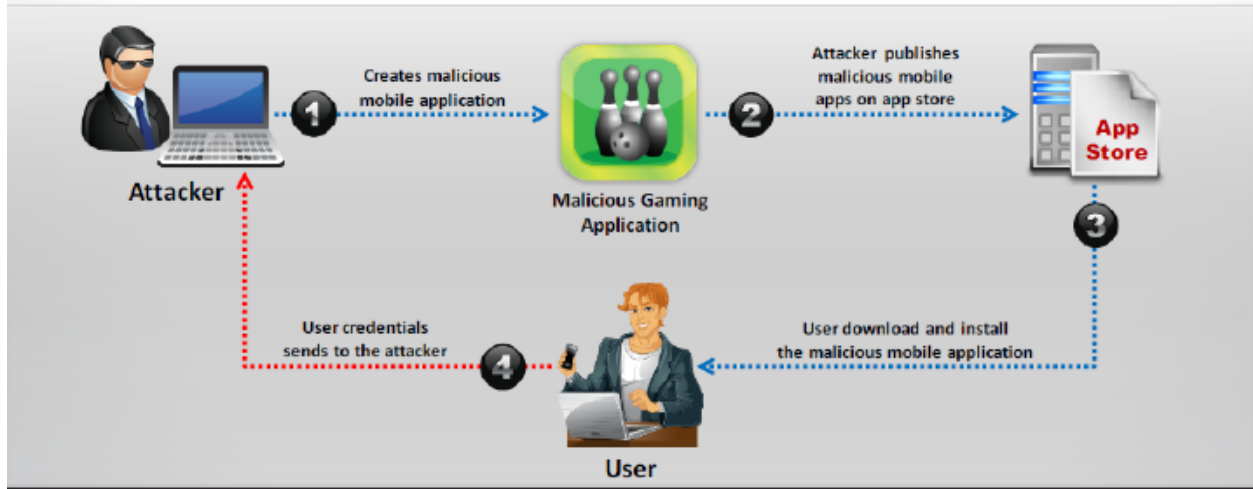
CEH
Certified Ethical Hacker



Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**



Unaware **users download these apps** and get infected by malware that sends **credentials to attackers**



কিভাবে সোশ্যাল ইঞ্জিনিয়ারিং আক্রমণ থেকে রক্ষা পাওয়া যাবে?

১. প্রত্যেক কর্মীকে কম্পানি পলিসি এবং প্রসিডিউরগুলো ভাল করে বুঝিয়ে তারপর কর্মীর কাছ থেকে সাইন নিতে হবে।
২. পাসওয়ার্ড পরিবর্তন পলিসি ডেপলয় করতে হবে।
৩. কম্পানির অপ্রয়োজনীয় কাগজগুলো ফেলে না দিয়ে নষ্ট করে দিতে হবে।
৪. এন্টিফিশিং টুলবার ব্যবহার করা যেতে পারে।
৫. ট্রেইনিং এর মাধ্যমে সবাইকে সতর্ক করা যায়। যেমন-

How to Detect Phishing Emails

1. Seem to be from a **bank, company, or social networking site** and have a **generic greeting**
2. Seem to be from a person listed in your **email address book**
3. Gives a sense of **urgency or a veiled threat**
4. May contain **grammatical/spelling mistakes**
5. Includes links to **spoofed websites**
6. May contain **offers that seem to be too good to believe**
7. Includes **official-looking logos** and other information taken from legitimate websites
8. May contain a **malicious attachment**

