**강현구 - 스미싱 예방 서비스**

고민점 : 이게 교수님이 희망하는 팀 프로젝트 주제가 맞을까..?

* 한번 교수님께 여쭤보는 게 좋을듯..?

**Project Aim**

The aim of the term project is to put the practical knowledge obtained during the course to an actual use. Any project topic is acceptable, as long as it directly touches on the theme of ethics.

* You can develop an app (e.g., Ethical Decision Making [AppStore](https://apps.apple.com/us/app/ethical-decision-making/id799710217), [Google Play](https://play.google.com/store/apps/details?id=com.mcae.decision&hl=en)).
* You can write tools/frameworks that promote/implement certain ethical issues (e.g., secure deep learning using homomorphic encryption) and evaluate it empirically.
* You can design a human experiment about a topic related to ethics (e.g., something akin to The Moral Machine).

Choices are endless, but it has to involve some technical depths. There will be an opportunity to present the initial ideas and get feedback (Project sales pitch sessions).

* 기술적인 깊이…? ⇒ 어느 방향으로의 기술적인 깊이?
  + 서버 / framework 개설?
  + AI 모델 등 개발?
  + ⇒ 다음주 월요일 수업 이후에 가볍게 여쭤보기

**Idea : 스미싱 예방 서비스**

* **정의**
  + 스미싱(Smishing) / 메신저 피싱 은 휴대전화의 문자 메시지나 SNS 서비스를 통해 개인정보를 탈취하고 재산상 이익을 취하는 사기 행각이다.
  + 앞으로는 스미싱으로 워딩을 통일하겠음
* **현황**
  + 스마트폰의 대중화로 인해서 현대 범죄의 양상이 크게 바뀌었다.
    - 더 이상 강도나 절도 같은 접촉을 통한 범죄보다, 인터넷과 통신 기술(ICT)을 이용한 ‘사기’와 ‘인터넷 사이버 범죄’들이 급격하게 증가하고 있다.
* **그 중에서 문자를 통한 사기 - 메신저 피싱 또한 급격한 증가세를 보인다**
  + 메신저 피싱 발생 수는 2020년 전후로 급격한 증가세를 보였다.
    - 경찰청 통계에 따르면 2019년 2,963건 발생하였으나, 2020년에는 4.5배 규모인 13,224건이, 2021년에는 17,841로 빠르게 증가하고 있다.
  + 메신저 피싱 연도별 피해금액 또한 2020년 587억원에서 2021년 1,265억 원으로 크게 늘어났다.
    - 2021년 기준 메신저 피싱 1건당 피해금액은 709만원이다. #

**해결 방안 분석 - 통계 출처 : Ahb Lab**

* **대부분의 스미싱의 사례는 일상생활과 밀접한 산업군을 사칭하는 경우가 대다수였다.**
* **대부분의 유도 방법으로는 전화 / URL / SMS / 카카오톡 순으로 나눠진다.**
  + 전화, SMS, 카카오톡의 경우 카카오톡 친구 추가 등을 통해 개인정보와 금융 정보 탈취를 목적으로 한다.
  + URL의 경우 오픈 카카오톡이나 피싱 사이트로 연결시키거나, 악성 앱을 다운로드 시켜 개인 정보를 유출시킨다.
* **대부분의 스미싱을 예방하는 수칙으로 URL을 클릭하지 않을 것을 꼽는다. (아래 예시)**
  + 메시지 본문에 포함된 URL을 클릭하지 않는다. 아직까지 대다수 피싱 문자는 본문에 URL을 포함하는 형태이다. 띠라서 신뢰할 수 없는 URL을 클릭하지 않는 것만으로도 피싱으로 인한 피해를 어느 정도 예방할 수 있다.
  + 의심스러운 문자의 발신자 번호를 인터넷에 검색한다. 대부분의 피싱 문자는 발신자 번호가 인터넷에서 정상적으로 검색이 되지 않기 때문에 인터넷 검색을 통해 예방할 수 있다.
  + 본문에 [국제 발신], [국외 발신]과 같은 단어가 존재한다면 피싱 문자를 의심해볼 만하다. 많은 피싱 문자가 국제 발신을 통해 발송되기 때문이다.
  + 카카오톡 친구 추가를 요구하거나 밴드 오픈 채팅방으로 연락하라는 내용의 문자도 피싱 문자일 확률이 높다. 메시지 본문에 URL을 첨부하는 수법은 이미 널리 알려져 공격자도 URL을 직접 전송하기 보다는 오픈 채팅방으로 유인해 악성 앱을 설치하도록 하는 수법을 많이 사용하고 있다. 따라서 오픈 채팅방으로 유도하는 문자도 주의해야 한다.
* **단, 실제로 도움이 되는 URL 인지, 사기와 관련된 URL 인지 사전에 확인할 방법이 마땅치 않다.**
  + (고민점) 흐으으음.. 이걸 기술적인 깊이가 있다고 할 수 있을까?
  + **⇒ 이 부분에 대해서 도움을 줄 수 있다면, 사기 예방에 도움이 될 수 있지 않을까?**

**해결책**

* **스미싱 사례인지 detection 하기**
  + 1. AI 모델로 학습
    2. Q. 굳이 AI 모델을 통해서 해결해야하나…? 학습 데이터나 이런 것을 구하기가 어려울 것 같은데..?
  + **2) Rule base 로 검토 ⇒ 이게 효율적이고 현실적인 방안일듯**
    1. ex)- 신원을 확인할 수 없는 URL 제공
       - 단축 URL 경우 원본 주소를 확인하는 방안이 있음
         * <https://forbes.tistory.com/1118>
       - **[Q - How?]** 사전에 신뢰할 수 있는 홈페이지 링크 쭉 추가해둔 다음, 거기에 해당하지 않으면 reject 하도록
         * 또는 구글 등으로 검색해서 얻은 링크와 비교하기
    2. ex)- 개인 정보를 요구함
    3. 등등

**기존 방안**

* 시티즌 코난 : 휴대폰에 악성 앱이 설치되어 있는지 점검