SOUPS'22-Ziboei-Do Password Managers Nudge Secure (Random) Passwords?

大概述：(S)Random Password Generator 生成随机口令，由PM存储，可以减轻口令重用的风险，研究基于浏览器的PM在口令创建时提供Nudge帮助促进随机口令的使用，但仍有许多用户不使用；(T)本文旨在探索如何将nudge的设计可以更有效地促进随机口令的使用。(A)对来自MTurk的558人进行了用户调研，首先隐藏自己的实验目的，要求参与者(3组，使用Chrome，Firefox和Safari)进行注册，并填写个人信息，统计注册过程中是否注意到了nudge，是否使用过随机口令生成器和PM等并使用卡方检验来看这些因素与随机口令的采用和是否存储的关系；(R)结果发现Safari的促进效果最好，使用过随机口令生成和注意到nudge对使用随机口令生成有显著影响，但使用PM的经历无明显影响；并探究不使用口令生成的原因

优点：① 研究了行为学中的nudge在PM的随机口令生成功能的应用情况，动机较好

② 实验方法的细节描述的较为详细，包括了实现步骤，人员来源和问卷内容

③ 介绍了实验方法的局限性和本文的未来工作

问题：① 表与的部分结果应进一步挖掘，如采用随机口令生成是因为该网站只用一次等

② "在PM中存储口令是第二主要的功能"，该说法无依据，不严谨

③ 作者应更详细描述：如何保证创建的PM与实际应用的PM现象和行为一致

④ 本文未给出改进这些问题的建议(只提到Chrome，Firefox可借鉴Safari)

---

1. 口令管理器的采用率不高，而其中的随机口令生成功能只有少部分人使用。
   nudge技术可以在不限制用户选择的情况下影响PM及其独特性的采用率。
2. 研究问题
   1) 引基于浏览器的PM在推动用户采用随机口令方面比较如何？
   2) 网站口令策略对随机生成口令的采用率的影响。
   3) 影响随机生成口令和在PM中存储口令的因素是什么？
   4) 用户(不)使用随机生成口令的原因是什么？

3. 研究方法。
   1) 三个浏览器nudge的区别：
   ① Chrome 当点击口令域会弹出nudge，包括"使用推荐口令"及15个字符的随机生成的串。提示用户Chrome为将口令保存到Google帐户中。
   ② Firefox 与Chrome类似但提示"使用安全口令"及Firefox将为此网站保存口令
   ③ Safari 采用了default nudge的方法，默认选中了生成随机口令的选项，并将18字符的口令填充到对应字段，提示用户创建了强的口令并且可以在所有设备上自动填充。
   2) 研究结构：(设计了网站，并在各个浏览器仿真各个PM的功能) → 经过了和何的Research Ethics Board的批准
   ① First consent form：提供给用户一个伪装的实验目的(不揭示password和nudging)
   ② Account registration：让用户使用邮箱和口令注册，可以选择自动生成的口令或自己的口令
   ③ 注册后问卷：询问用户有关身份的5个问题
   ④ 登录：使用注册的邮箱和口令登录网站
   ⑤ 研究后问卷：询问参与者有关nudge，PM和口令创建的问题
   ⑥ Second consent form：在提交前向用户解释实验的真正目的

   3) 实验规则：
   ① 用户只能提交1次数据，保证数据质量。② 只有用户提交两个表单时才允许收数据出于道德考虑
   ③ 未收集邮箱，只收集3次保证匿名性
   4) 分析的因素和方法
   ① 随机生成口令的采用率的区别；3个浏览器；3种口令策略；对观察到nudge与未观察到nudge的参与者；之前使用过和未使用过PM的参与者；之前使用过和未使用过随机口令生成器的PM；在实验中使用日常用的浏览器的参与者和使用非日常使用的参与者
   ② 在PM中保存口令的rate的区别：3个浏览器，对观察到nudge与未观察到nudge的参与者
   ▲方法：使用 χ^2 test来辨别哪些影响因素是关键的
   对于开放式问题，采用emergent coding approach进行分析，使用Cohen's kappa判断几个研究人员的结果是否一致。

4. 结果。
   1) 参与者中去除了3位未通过attention check的，共558份响应，191 Chrome，188 Firefox，179 Safari
   2) 所有使用随机口令生成器的参与者都将口令存储在PM中
   3) 使用随机口令生成的原因：19.89% convenience，12.19% security，5.56%存储特征
   不使用的原因：23.66%又注以记忆，11.47%更愿意自己选择

5. 讨论。
   1) Safari中随机生成口令采用率较高的原因分析：
   ① 颜色和弹框更突出，而且可以自动填充生成的口令(提示用户口令强度strong)
   ② 在弹出的消息中包含存储和在不同设备中autofill(对不熟悉PM的用户更友好) → 即同步功能
   ③ 采用了default nudge，更有效。
   ④ 隐藏了最后6个字符，可以防止肩窥攻击，更安全
   2) 局限性
   ① 本实验为quasi-experiment，用户不是随机分配到各个browser，故用户行为的区别可能是浏览器用户之间的区别
   ② Amazon MTurk的数据缺乏样性且数据质量差
   ③ 参与者可能不熟悉英语，存在一定的语言和文化偏差，以及social desirability bias
   ④ 部分用户使用了第三方的口令生成工具