Contents

1. What is wrong?

2. UI of Security

3. HCI Issues

4. Usability Design
1. What is wrong?
1. What is wrong?

The 10 Biggest Tech Failures of the Last Decade

Windows Vista Tip: Disable annoying "Need your permission to continue" prompts

By Gina Trapani, 8:30 PM on Thu Jan 25 2007, 413,031 views

Windows Vista’s User Account Control security "feature" - which I like to call Sir Obnoxious Naggy McNag - is bound to drive any power user batty within an hour of downloading, installing and configuring your favorite programs. If you hate Vista for asking you every single time you try to do something if you’re sure you want to, then disable User Account Control. The How-To Geek’s got the details:
1. What is wrong?

- Lack of understanding for users and tasks
  - Fail to provide users’ psychological acceptance
  - Fail to provide usable security
- Users care only their tasks, not security
  - Security is not a task goal
  - Often interfere with usability
- Additional effort, cost to comply
  - Too complex, too difficult
2. User Interface of Security
### How secure is enough secure?

- Fail to provide users’ trust in Internet banking

<table>
<thead>
<tr>
<th>Measures</th>
<th>Type</th>
<th>Threat</th>
<th>HCI Issue</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID/PW</td>
<td>User knows</td>
<td>Dictionary Attack</td>
<td>Memory</td>
<td>User Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social Eng.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td>User has</td>
<td>Hacking</td>
<td>Theft, Lost</td>
<td>PC/USB</td>
</tr>
<tr>
<td>PW for PKI</td>
<td>User knows</td>
<td>Dictionary Attack</td>
<td>Memory</td>
<td>User Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social Eng.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Card</td>
<td>User has</td>
<td>Hacking ?</td>
<td>Theft, Lost</td>
<td></td>
</tr>
<tr>
<td>OTP</td>
<td>User has</td>
<td>–</td>
<td>Theft, Lost</td>
<td>–</td>
</tr>
<tr>
<td>Secret Number</td>
<td>User knows</td>
<td>Dictionary Attack</td>
<td>Memory</td>
<td>User Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social Eng.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q: I have 30 active ID for e-banking(2), e-trading(1), mail(5), cafe(2), websites (20+). Can I comply with these guidelines?

- **Task Requirements**
  - Remember 30 pseudo-random passwords
  - Change every other 3 months
  - No not take memo

Human cannot cope to security!
HCI Issues: ID/PW

- Password authentication survey (HFES, 2009)
  - Users record on sticker 15-20%
  - Enterprise users record on notebooks (66%), computer file (55%)
※ 1% PW among 3,200 Million PW 1% 123456 (Imperva, 2010)
HCI Issues: Security Patch

- Different perception between security and other update
  - Window update, security patch, agreement (20% compliance)
  - Game patch, no agreement (100% compliance)
- Automatic security patch downloads for Hangame
  - Advanced agreements for automatic patch
  - 200 million patch clients for 16 days
- Users perception to security patch
  - Security is additional function, not key elements
HCI Issues: i-PIN

- Difficult to change users behavior
  - SSN vs. i-PIN
  - Up to 8 Million copies from 2006

- High business risk in using SSN
  - Marking >>> Security
  - SKComs Case, $2,000 compensation for each
HCI Issues: PKI

- Enhancing technology not intrusive
  - Analogy to real world procedure
    - Seal or signature for cyber banking
- Convenient and cost effective
  - Immediate money transaction
- When security is user values
  - Mandatory for cyber banking and trading

Users will accept additional cost, only if security is users value.
HCI Issues: Complexity of Security Technology

- Complexity of System
  - Internal Complexity
  - External Complexity: Interface

- Complexity of security tech.
  - S/W: Vaccine, Anti-Spyware, etc.
  - H/W: F/W, IDS, Web F/W, IPS, etc.
HCI Issues: Culture and Environments

- Difficult to change culture, infra
  - Easy to adopt a new technical change, difficult to change business practice and culture
  - SSN is widely used for Internet Business
  - \( \rightarrow \text{e.g.) New standards for Industry: Km, m^2} \)

- Technology influences our culture
  - Privacy in using telephone in 1800s
  - Smartphone?
Bias perception of risk (Tversky and Kahneman, 1973)
- overestimate the value of their own experience if they have not been exposed, underestimate the risk
- overestimate the associate with news stories

“It can’t happen to me” bias (Christensen, 1987)
- Overconfident of their ability to avert accident
  e.g., 75–90% believe they are above average in driving skill

People will accept a higher level of risk (Slovic, 1978)
- if the level of risk is controllable, is known, and understood, and the consequence are immediate
Mental Model

- Explanation of one’s thought process about how something works in the real world
Cost of Compliance

- User will not use if the cost of compliance is high
  - Cost, effort, time etc.
Usability Design for Information Security

- New security technology will improve the level of security?
  - Cannot be without transforming the weakest link
  - User-Centered Design for Security Mechanism
    ※ 84% of Security Failure, Human Error (Deloitte, 2009)

- HCI
  - Information security is man–machine System
  - Trade-Off between usability and security
  - Need to understand users and their tasks

Security is only as good as it’s weakest link, and people are the weakest link in the chain