**Motivation**

- Users access many services through the web: forums, shopping, banking, mail, etc.
- Mostly password-based user authentication
- Users tend to reuse passwords [1]

→ Protecting passwords is crucial

**Problem Statement**

- Ideally web page with password field https protected and password transmitted using https
- But: On many web pages no https at all or only password transmission secured
- No browser warning in these cases

→ Passwords are often not adequately protected and users are not aware when this is the case

**Our Goal**

- Support users in detecting suboptimal condition for password entering
- Warn users with a mixture of passive and active warning method to avoid interruption and annoyance in case of login intention is expressed
- Provide understandable texts with recommendations on how to proceed

**Our Approach**

Highlighting password fields and displaying a non-blocking warning dialog only in case password field is focused

**Highlight Password Field**

- In [2], we showed that combination of red background and yellow warning triangle is well perceived as security warning in the considered scenario
- Password field might not be of type `password`
- Also: positive feedback for user
- Ideally individualized icon to prevent attacks

**HTTPS Available (short version)**

*It is insecure to enter a password here!*

Your password could fall into the hands of an unauthorized person and could be used to access your personal data [less]

You should always use a secure mode (https) to open this website by clicking on „HTTPS for this site“ [more]

More Information

HTTPS for this site Close warning

- Texts based on a (pre-)user study

**HTTPS Not Available (long version)**

*It is insecure to enter a password here!*

Your password could fall into the hands of an unauthorized person and [more]

This website does not provide a secure mode (https). In case you decide to log into this website anyway, you should at least use different passwords for different websites [less]

More Information

This website does not provide the option of entering and transmitting your password securely (via https). In case you use the same or a similar password on different websites, and if your password is intercepted on an unsecured website (e.g. this one), it can be used for other services as well [less]

Add an exception Close warning

- Future Work
  - Conduct a field study
  - Enhance Add-On: e.g.
    - Consider further field types, e.g. credit card information
    - Consider website type (e.g. online banking) to be more precise about the possible risks

**Literature and Related Work**


**Further Information**

secuso.informatik.tu-darmstadt.de/de/research/results/passsec-add-on/