

Internet safety

Dan Ionita

UTwente, Services and cybersecurity (scs.utwente.ewi.nl)

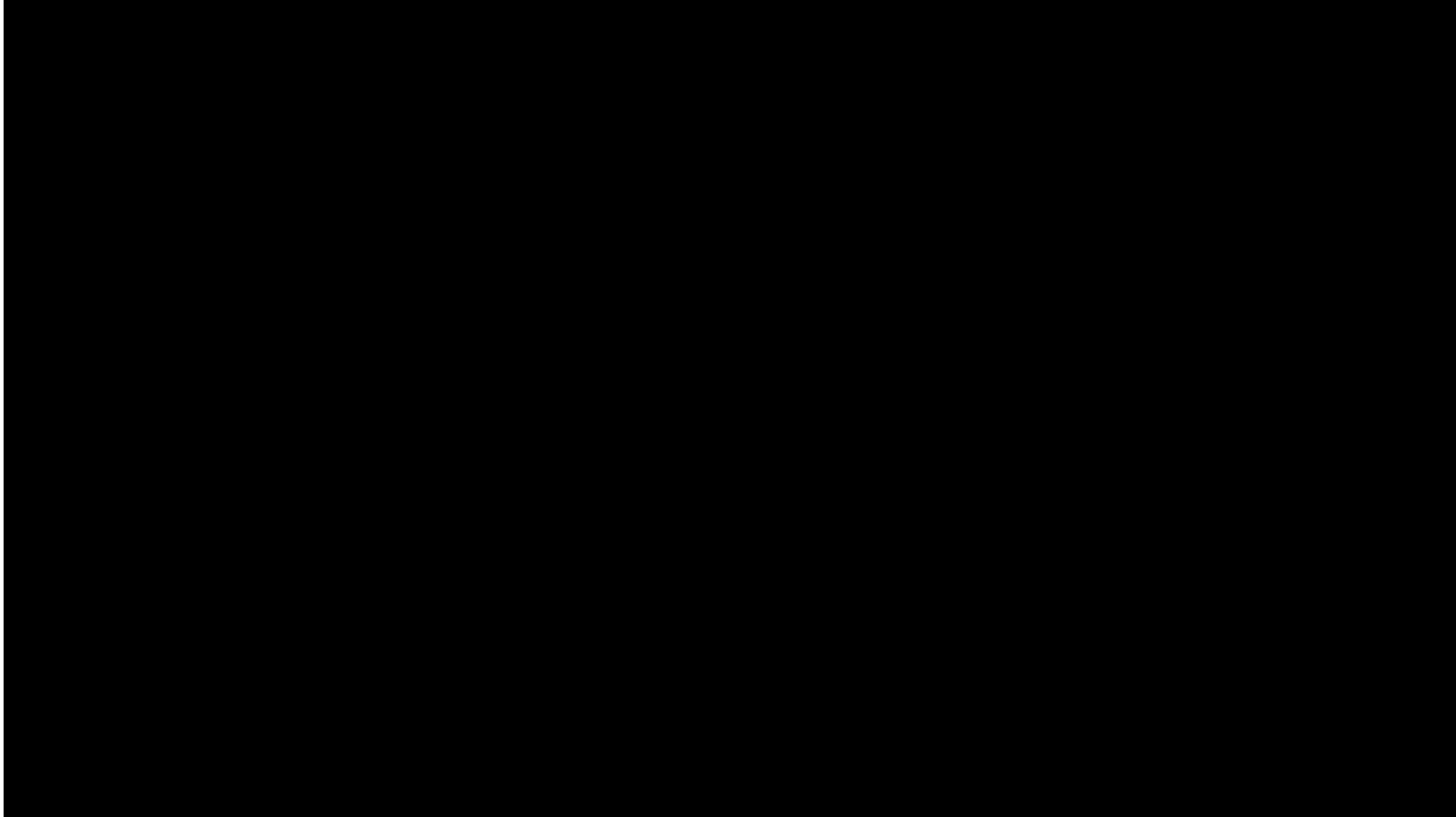
Internet fundamentals - quiz

- Go to <https://www.certifiedsecure.com>
- Start the “Internet fundamentals” challenge:



Internet Fundamentals
Start the Challenge

Internet fundamentals - video

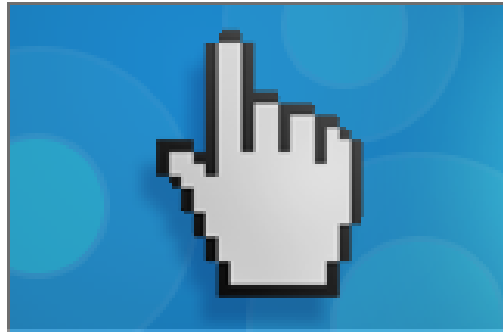


Internet fundamentals - quiz

- Now let's try again

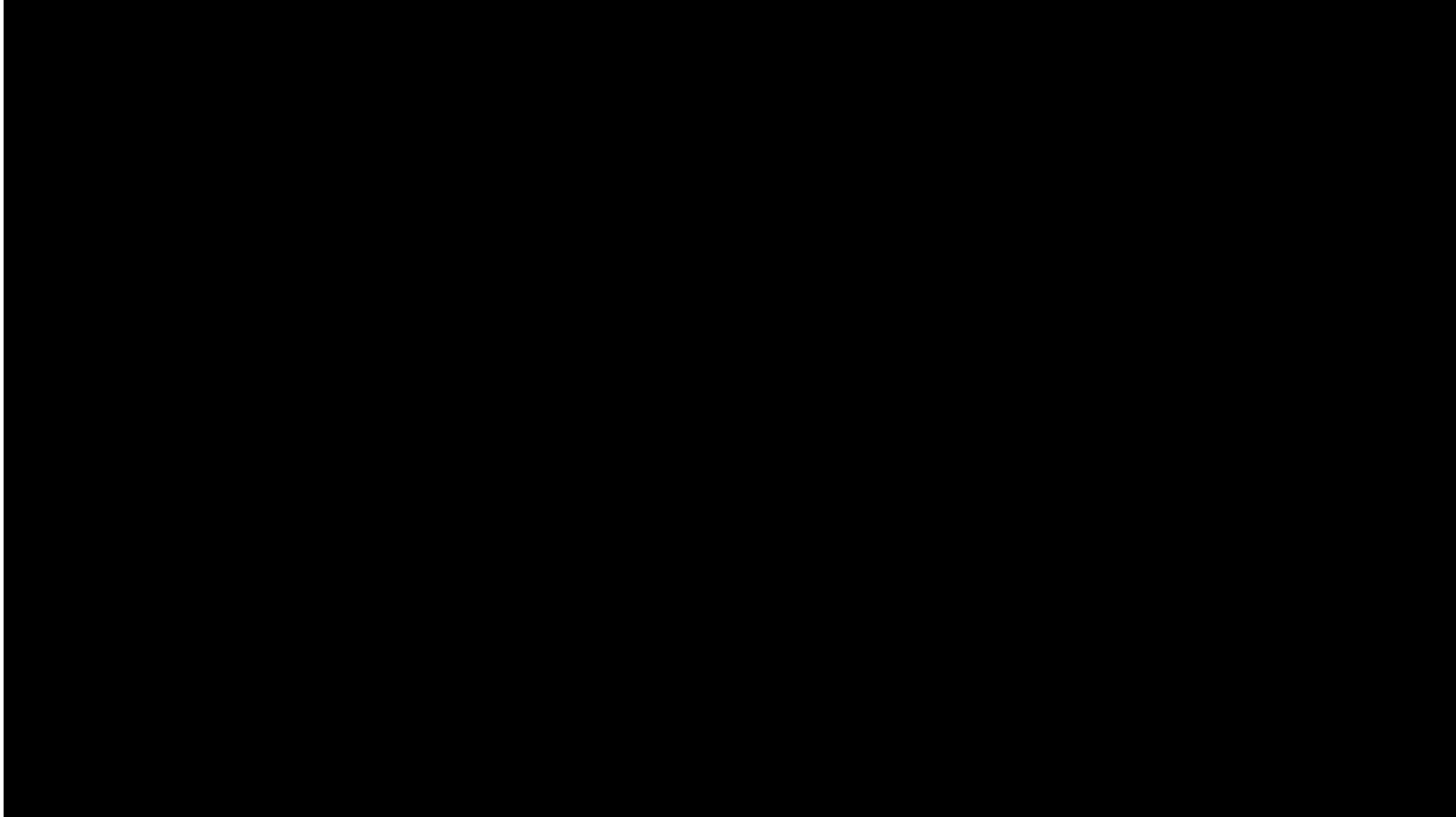
Phishing - quiz

- Go to <https://www.certifiedsecure.com>
- Start the “Don’t click” challenge:



Don't click
Start the Challenge

Phishing - video



Phishing - quiz

- Now let's try again

Safe internet - challenge

- Let's do the "Safe Internet Challenge" together
- You can continue at home with Safe Internet Plus.
- And then continue to the more advanced security topics to learn hacking.

Personal privacy protection



Tips

- Keep software up-to-date
- Always check the URL
 - In the address bar
 - Under buttons and links
- Be VERY careful with attachments

- Never use weak passwords:
 - Never use a name, word, birthday, or combinations of these
 - Never re-use passwords
 - Change password after leaks (and check for leaks frequently!)
 - Password managers can help

- WiFi
 - Never enter any sensitive information (e.g. password) on a HTTP (not HTTPS) page while on public WiFi
 - Avoid navigating to sensitive websites while on public WiFi

Tips

- Web browsing:
 - Use privacy extensions: HTTPS enforcer + anti-tracker + unshortner + anti-malware
 - <https://www.privacytools.io/>
- Digital identity:
 - Keep profile details private
 - Use pseudonyms

Advanced:

- Anonymous browsing:
 - VPN, TOR
- Encrypting files:
 - BitLocker, VeraCrypt

Tools

- Anti-tracking:
 - Ghostery, Privacy Badger, Disconnect, some adBlockers.
- Force HTTPS:
 - HTTPS Everywhere
- Unshortners:
 - Unshorten.link, Ghostery
- Password managers:
 - LastPass, LogMeOnce
- Anti-malware
 - Malwarebytes, Windows defender
- Password manager
 - Lastpass, 1password