CENSUS
IT Security Works

EFFICIENT WI-FI PHISHING ATTACKS

GEORGE CHATZISOFRONIOU

sophron@census-labs.com
www.census-labs.com

> WI-FI PHISHING PROCESS

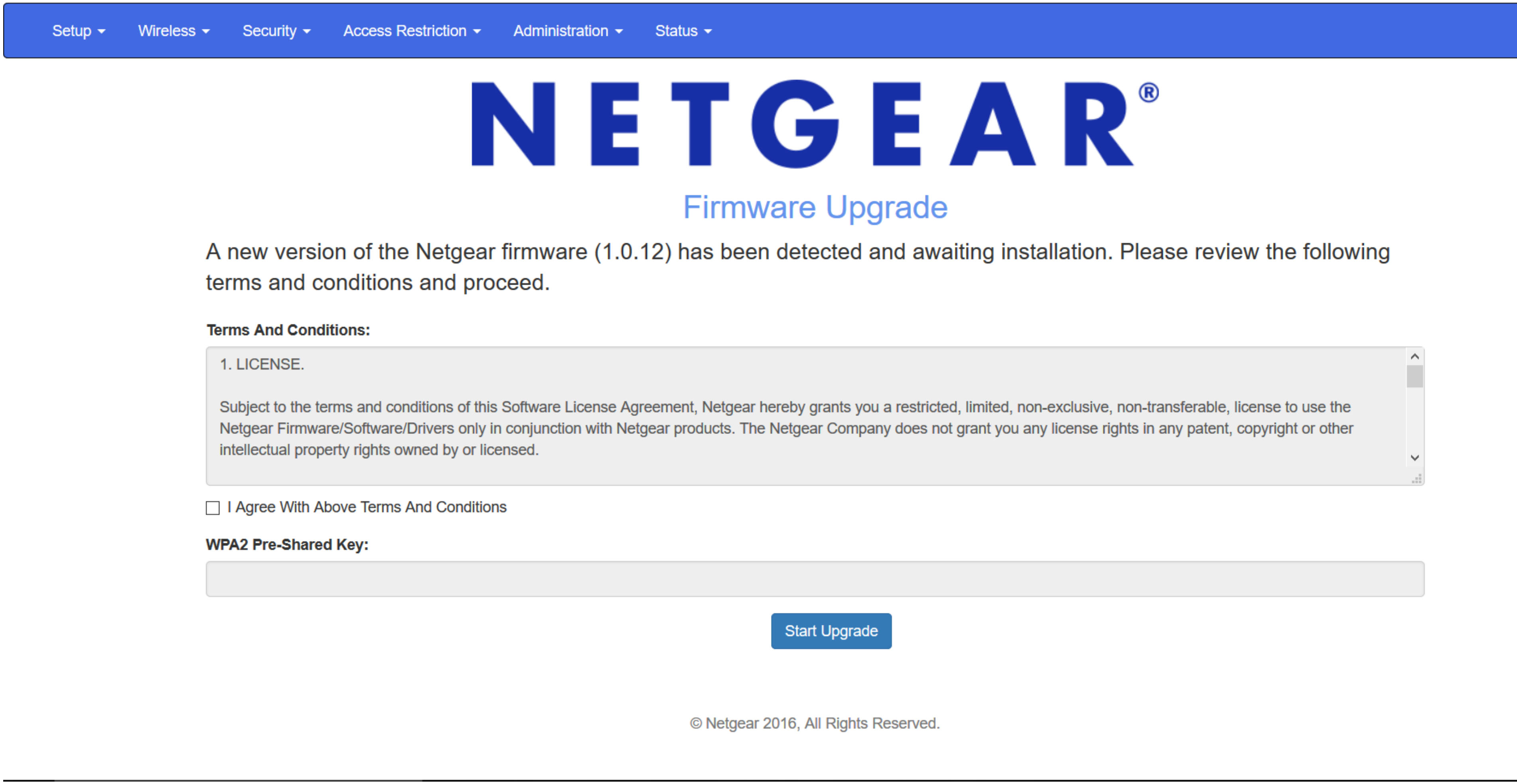
1. Evil Twin (or KARMA) to get MiTM
   - DEAUTH or (physical layer) jamming attacks to disrupt existing associations
2. Redirect to fake website
   - Credentials capture or malware infection

> WPA/WPA2 PSK PHISHING

- WPA2 PSK brute-forcing remains time-consuming
  - PBKDF2 with 4096 iterations & network’s ESSID as salt
  - 1 GPU (80000 pwds/s) needs 30 days to break an 8-char PSK
- WPA2 phishing to the rescue!

> VICTIM PROFILING

- 802.11 Beacon frames (Physical layer)
  - ESSID
  - BSSID (discloses the router’s vendor)
    - e.g. If BSSID starts with "00:12:17“, the frame was broadcasted by a Linksys router
  - Encryption type
- HTTP User-Agent header (Application layer)
  - OS
  - Browser



Firmware Upgrade

A new version of the Netgear firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

Terms And Conditions:

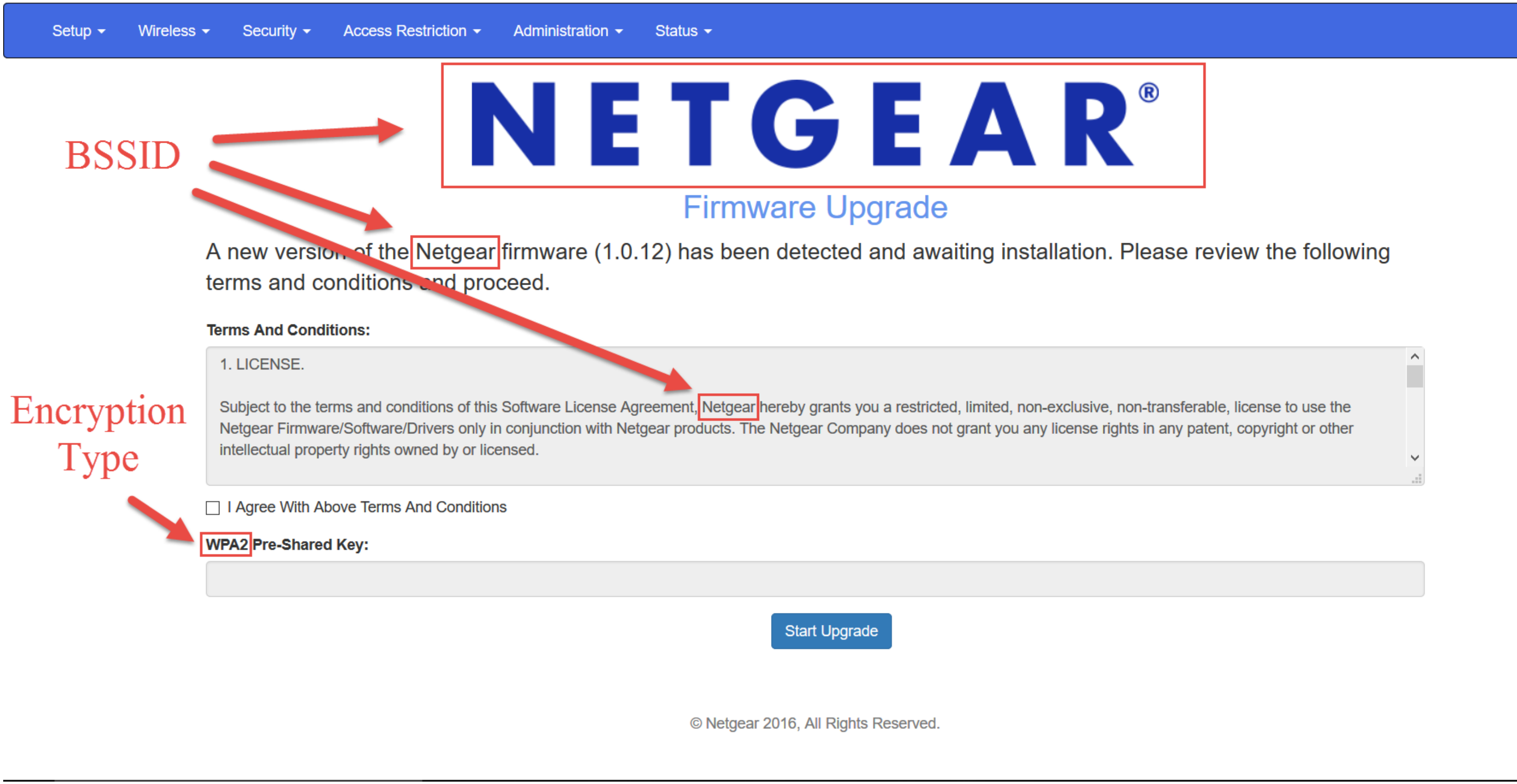
1. LICENSE.

Subject to the terms and conditions of this Software License Agreement, Netgear hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Netgear Firmware/Software/Drivers only in conjunction with Netgear products. The Netgear Company does not grant you any license rights in any patent, copyright or other intellectual property rights owned by or licensed.

□ I Agree With Above Terms And Conditions

WPA2 Pre-Shared Key:

© Netgear 2016, All Rights Reserved.



BSSID

Firmware Upgrade

A new version of the Netgear firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

Terms And Conditions:

1. LICENSE.

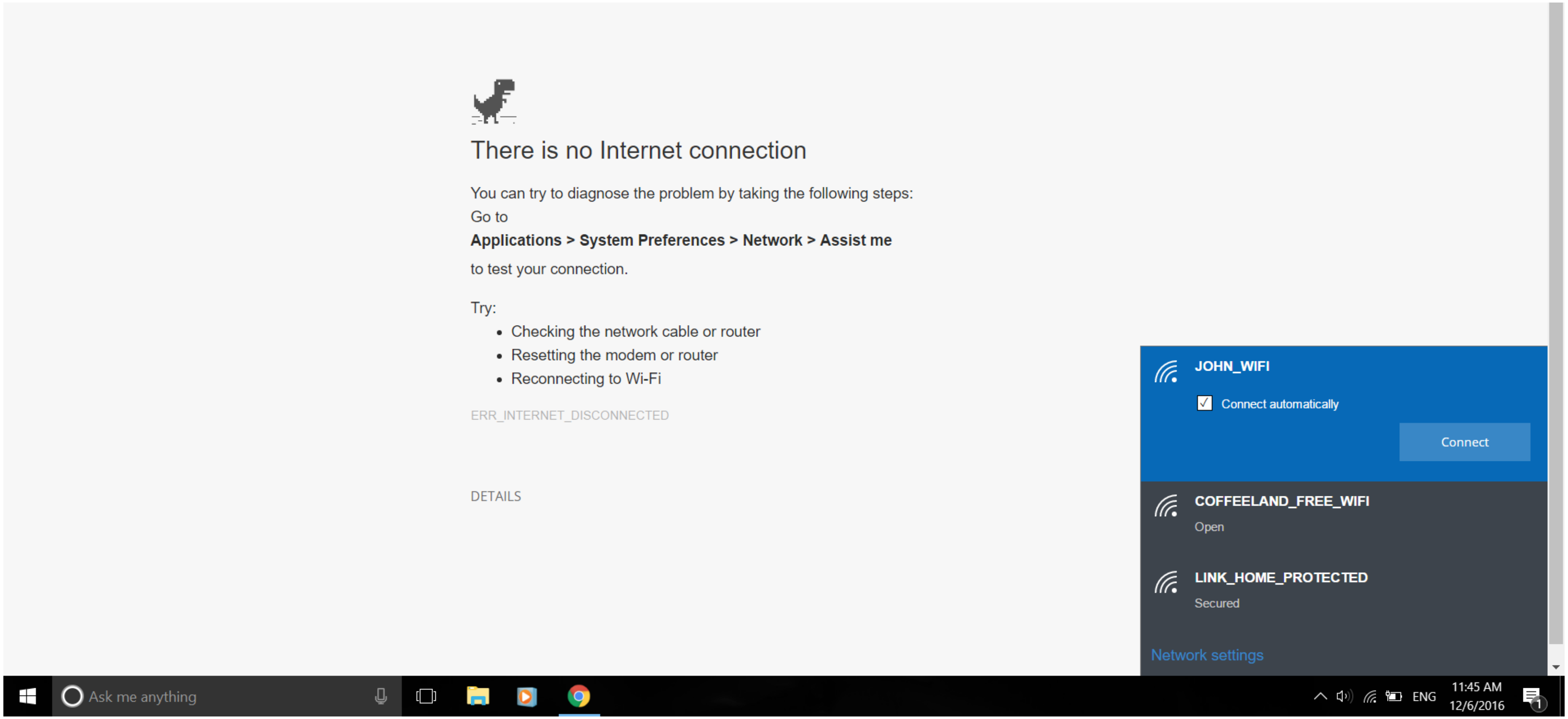
Subject to the terms and conditions of this Software License Agreement, Netgear hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Netgear Firmware/Software/Drivers only in conjunction with Netgear products. The Netgear Company does not grant you any license rights in any patent, copyright or other intellectual property rights owned by or licensed.

Encryption Type

□ I Agree With Above Terms And Conditions

WPA2 Pre-Shared Key:

© Netgear 2016, All Rights Reserved.



There is no Internet connection

You can try to diagnose the problem by taking the following steps:
Go to
Applications > System Preferences > Network > Assist me
to test your connection.

Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

ERR_INTERNET_DISCONNECTED

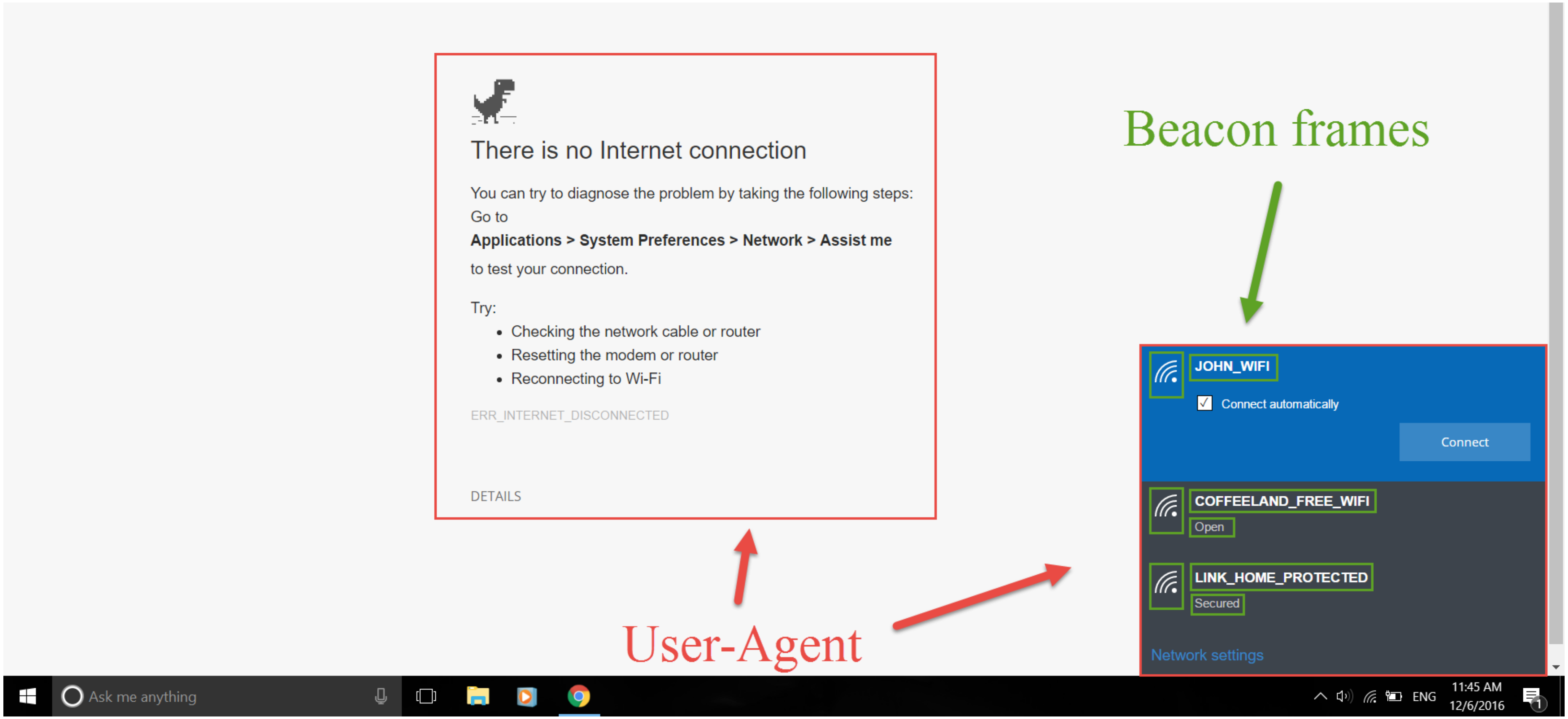
DETAILS

JOHN_WIFI
☑ Connect automatically
Connect

COFFEELAND_FREE_WIFI
Open

LINK_HOME_PROTECTED
Secured

Network settings



There is no Internet connection

You can try to diagnose the problem by taking the following steps:
Go to
Applications > System Preferences > Network > Assist me
to test your connection.

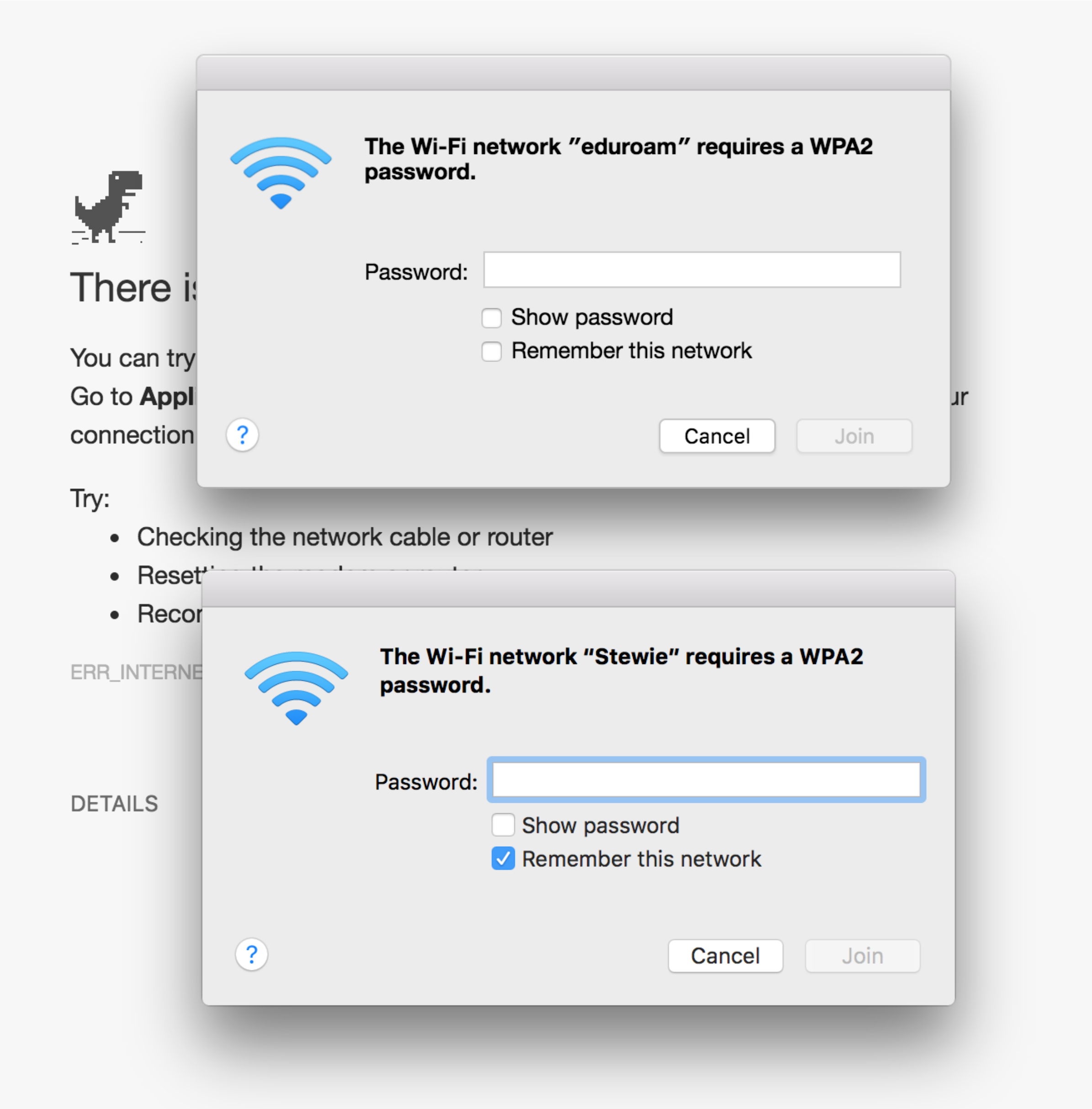
Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

ERR_INTERNET_DISCONNECTED

Beacon frames

User-Agent



The Wi-Fi network "eduroam" requires a WPA2 password.

Password:

□ Show password

□ Remember this network

The Wi-Fi network "Stewie" requires a WPA2 password.

Password:

□ Show password

☑ Remember this network

> Wifiphisher v1.2

- Automates the process for effective Wi-Fi phishing attacks based on victim info
- Features a template engine for easy customization
- https://wifiphisher.org

Thank you!

CENSUS

IT Security Works