Everybody’s life: phishing emails
The Common Belief ...
... May Need to Be Revised?
Research Question 1

What traditional phishing frameworks have been reported in literature, and compared to our approach, what are their features and limitations?
Limitations in Existing Phishing Frameworks...

+ data collection
  email reports
  guiding assistants

- lack of accuracy and recency
  hard to maintain back-end
  no continuous tracking
  complex setup
... are the Features in Our Phishing Framework

+ data collection
  - email reports
  - guiding assistants
    - no assistants required

+ lack of accuracy and recency
  - easy
  - hard to maintain back-end
  - no continuous tracking
  - complex setup
    - no setup required
Research Question 2

What is phishing on demand, how are the features implemented, and what is the new threat we identified?
Phishing on Demand

1. tracking user actions
2. user data
3. Track input & mapping
4. apply user input
5. rendering web page
6. screenshotting
7. screenshot & metadata
8. rendering image (…)

client

HTTP server

headless web browser
client

(phishing) server
Feature: Native Textboxes
Feature: Native Textboxes

WORKS ALSO ON TOUCH DEVICES!
Feature: Native Hyperlinks
Feature: Live Feedback
Feature: Pop-up Windows
Feature: Ad-blocking
Feature: Logging

963120 [http-nio-8080-exec-8] INFO ch.baesi.bachelorthesis.phish.Phisher - user: 1
964363 [http-nio-8080-exec-6] INFO ch.baesi.bachelorthesis.phish.Phisher - user: 1
964363 [http-nio-8080-exec-6] INFO ch.baesi.bachelorthesis.phish.Phisher - Pressed Key(s): [Shift]
964801 [http-nio-8080-exec-1] INFO ch.baesi.bachelorthesis.phish.Phisher - ---------------------------------------------------------------
964814 [http-nio-8080-exec-1] INFO ch.baesi.bachelorthesis.phish.Phisher - user: 1
964814 [http-nio-8080-exec-1] INFO ch.baesi.bachelorthesis.phish.Phisher - Pressed Key(s): [S]
964814 [http-nio-8080-exec-1] INFO ch.baesi.bachelorthesis.phish.Phisher - ---------------------------------------------------------------
966017 [http-nio-8080-exec-9] INFO ch.baesi.bachelorthesis.phish.Phisher - user: 1
966017 [http-nio-8080-exec-9] INFO ch.baesi.bachelorthesis.phish.Phisher - Pressed Key(s): [R]
Feature: Simple Configuration

Required
backendBase=https://www.myphishingservice.com/
aureliaBase=https://www.myphishingservice.com/
entryPoint=https://www.bank.com/

Optional
debug=false
headless=true
mouseClickSleep=500
keyStrokeSleep=100
awaitBrowserSleep=400
adblock=true
(Mis)use in Practice
Example #1: Google
Example #2: E-Banking
Example #3: Two Factor Authentication
Demo
Research Question 3

Do users notice any differences in browsing using our approach, and if yes, which?
Covert Phishing Study

“Usability study” in disguise

Randomly ordered browsing tasks on regular and phished sites

Survey of knowledge and experiences
Findings

Usability feedback
- Websites updated their design
- Speed sometimes low
- Broken text/image synchronization
- “What did I do wrong?”

Phishing awareness
- Short tasks raised no concerns
- Broken tasks raised suspiciousness
A New Threat on the Rise?

NO

lower speed

limited reliability

YES!

no template changes required

(almost) any page can be phished

fully supports 2FA

raises no suspicion
TRY IT OUT YOURSELF!

phish.anotherlogin.com
Summary

... are the Features in Our Phishing Framework

- data collection
- email reports
- lack of accuracy and recency
- easy trend to maintain back-end
- rendering assistants
  - no assistants required
- continuous tracking
  - no setup required

Example #3: Two Factor Authentication

Phishing on Demand

Findings

Usability feedback
- Websites updated the design
- Speed sometimes low
- Broken text/image synchronization
  "Did I just break the site?"

Phishing awareness
- Short tasks raised no concerns
- Broken tasks raised suspiciousness