ETH zürich

A Strategy to Handle Phishing Attacks against Universities

TNC 2014

What is phishing?

Phishing is the application of “social engineering” messages to trick victims into revealing personal information, such as the details of user-accounts, bank accounts or credit-card numbers.

Why do criminals send phishing messages?

Money: $6 billion in financial losses from phishing in 2013

Why do criminals send “User-Account” phishing messages?

- Mass-collection of user accounts
- To send mail using legitimate mail providers
- To avoid IP-blacklists & other forms of filtering

Why are universities a target for user-account phishing?

- We have a large pool of inexperienced users
- We are unlikely to black-list other universities

Phishing Attacks

- Difficult to stop using traditional mail filtering …
- They can come from external sources or *accounts within your university*
- We experience several attacks per day

Methods used by “university” phishers.

- Generic phishing messages (e.g. “mailbox quota“ & “PayPal account”)
- They study our web pages and send messages using the names of specific persons or offices
- They use copies of our login pages

Sehr geehrter Nutzer,

Ihr Zugang zu Veranstaltungskalender läuft bald ab, daher müβen Sie es sofort wieder zu aktivieren oder es wird automatisch geschlossen. Wenn Sie beabsichtigen, diesen Service in Zukunft zu nutzen, müssen Sie Maβnahmen auf einmal zu nehmen! Um Ihr Konto zu aktivieren, besuchen Sie die folgende Seite und loggen Sie sich mit Ihrem Uni-Account. Nach der Anmeldung wird Ihr Konto wieder aktiviert und es wird Sie zu Ihrem Veranstaltungskalender umzuleiten. Login-Seite:

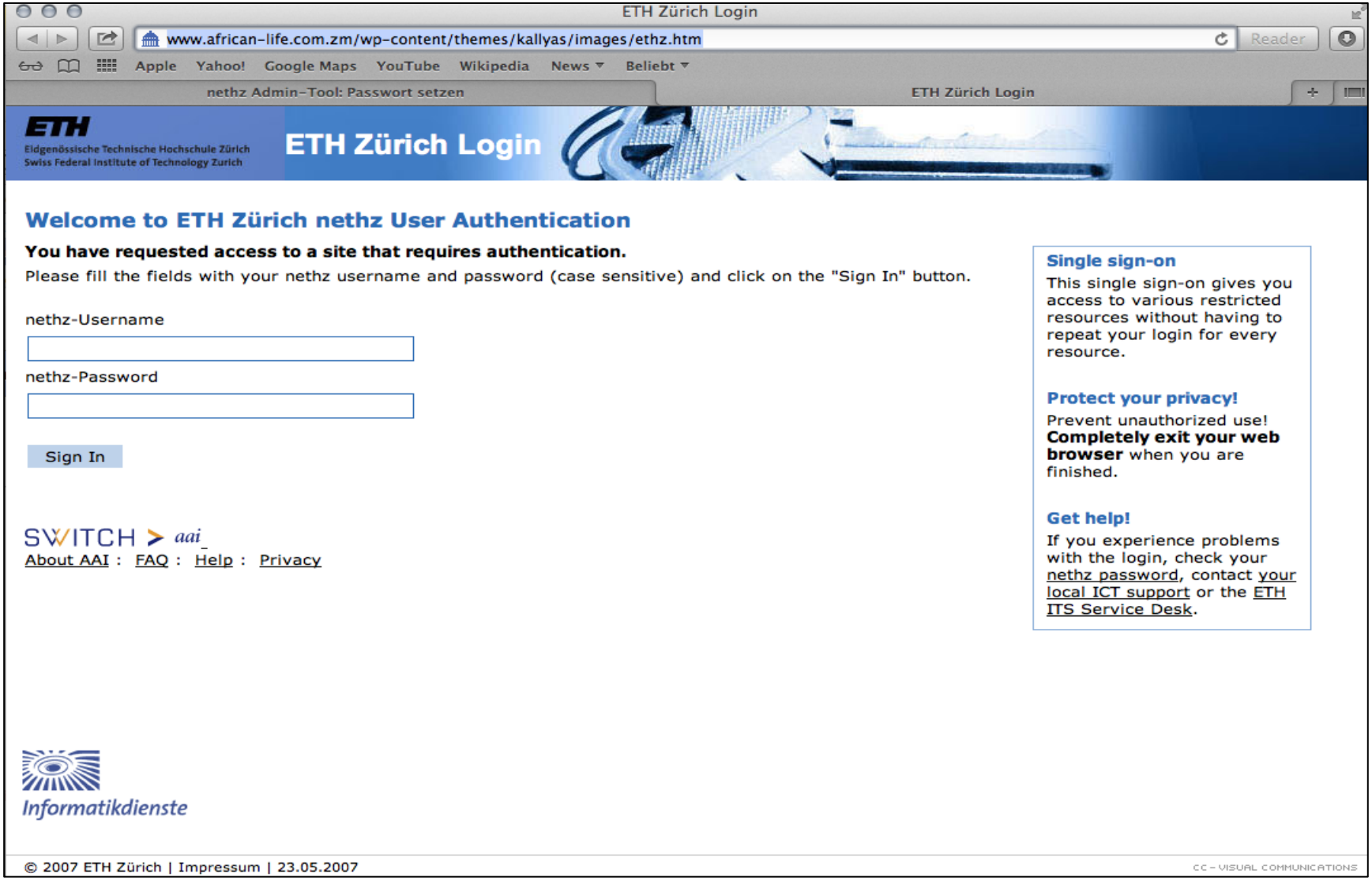
"http://www-vk-ethz-ch.eduk.tk/Veranstaltungskalender/ loginPre.do3lPfYjMm4fpya90PsmqoYiH8n/"

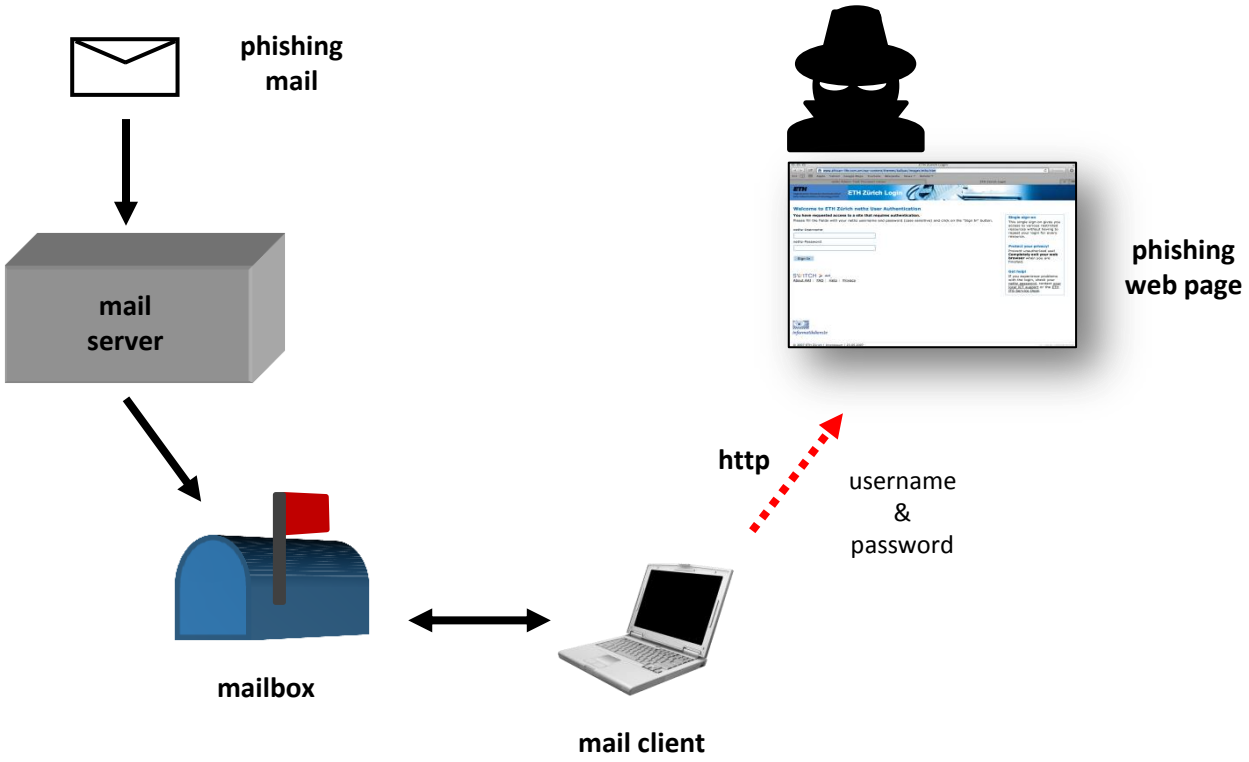
http://www.vk.ethz.ch/Veranstaltungskalender/loginPre.do3lPfYjMm4fpya90PsmqoYiH8n/

Wenn Sie sich nicht anmelden können,
wenden Sie sich bitte an peter.bircher@id.ethz.ch

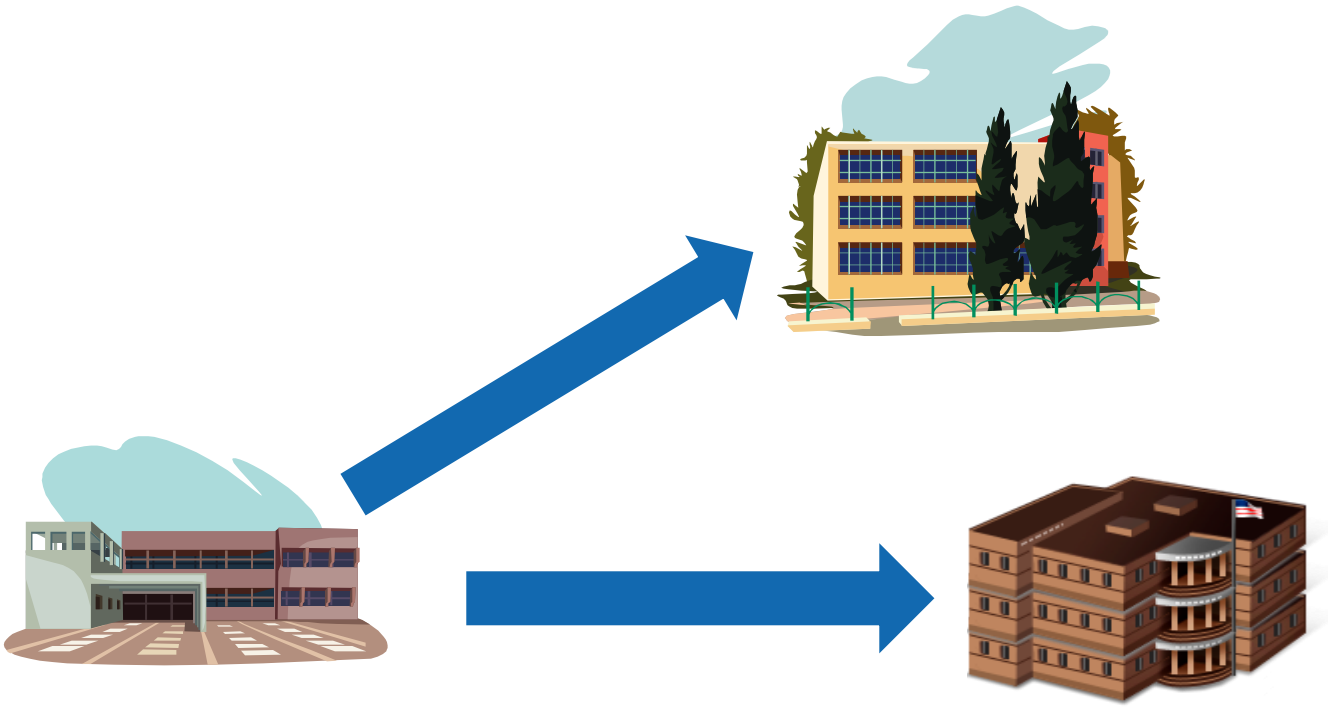
Mit freundlichen Grüβen,

Peter Bircher
ETH Zürich
ID Basisdienste
WEC E 22
Weinbergstrasse 11
8092 Zürich
Telefon: +41 44 632 72 13
E-Mail: peter.bircher@id.ethz.ch


ETH Zürich Login
www.african-life.com.zm/wp-content/themes/kallyas/images/ethz.htm
Reader
Apple Yahoo! Google Maps YouTube Wikipedia News Beliebt
nethz Admin-Tool: Passwort setzen
ETH Zürich Login
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
ETH Zürich Login
Welcome to ETH Zürich nethz User Authentication
You have requested access to a site that requires authentication.
Please fill the fields with your nethz username and password (case sensitive) and click on the "Sign In" button.
nethz-Username
nethz-Password
Sign In
SWITCH aai
About AAI : FAQ : Help : Privacy
Single sign-on
This single sign-on gives you access to various restricted resources without having to repeat your login for every resource.
Protect your privacy!
Prevent unauthorized use! Completely exit your web browser when you are finished.
Get help!
If you experience problems with the login, check your nethz password, contact your local ICT support or the ETH ITS Service Desk.
Informatikdienste
© 2007 ETH Zürich | Impressum | 23.05.2007
CC - VISUAL COMMUNICATIONS


phishing
mail
mail
server
mailbox
mail client
http
username
&
password
phishing
web page

Criminals use universities to phish other universities



What do criminals do with “phished” accounts?

- Use them to send spam/phish/malware messages
- Use them to set up phishing web pages
- Hold some accounts in reserve for later use
- Sell accounts to other criminals

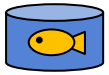
Countermeasures

- User education
- Inspection queues for suspected phishing messages
- Monitoring
- Neutralise phishing URLs
- User mailboxes
- Minimise reaction time

Countermeasures (1)

- User education
  - articles in campus newsletters & websites
  - phishing information web page
  - web page showing latest phishing messages

Countermeasures (2)

- Inspection queues for suspected phishing messages
  - inbound mail 
  - outbound mail
  - internal mail (on your own mail server)
  - labour-intensive
  - requires tools to efficiently list, display, release or delete messages

Countermeasures (3)

- Monitoring
  - inbound http traffic to find pages getting a large number of hits
  - outbound mail traffic to find users sending a large number of messages
  - inbound mail traffic to find users receiving a large number of bounce messages
  - automatic geo-tracing of logins to user accounts
  - we would like a 10-day log of outbound http traffic & a method to see which users responded to a phishing message

Countermeasures (4)

- Neutralise phishing URLs
  - Redirect a phishing URL to a warning web page
  - Block a phishing URL's IP-address

Countermeasures (5)

- User Mailboxes
  - Set a daily limit on the number of messages that can be sent by any user
  - Inform phishing recipients that their accounts may be “phished”
  - Lock accounts which are sending spam/phish/malware messages or hosting a phishing web page
  - Keep a password history to prevent "phished" users from re-using compromised passwords
  - Remove phishing messages from user mailboxes

Countermeasures (6)

- Minimise reaction time … by allowing your Helpdesk to
  - lock “phished” accounts
  - redirect phishing URLs

Collaboration

- Get advice from your NREN
- Exchange of experiences with other universities
- Perhaps some help from TERENA ?

Thank You