# Nettsikkerhet

Tom Heine Nätt
Høgskolelektor
Høgskolen i Østfold
tom.h.natt@hiof.no

# Plan

- Introduksjon
- Ulike teknikker
- Social Engineering
- Digitale fotavtrykk
- Identitetstyveri

# Introduksjon

Flere brukere

+

Raskt utviklende teknologi

+

Nye anvendelser

=

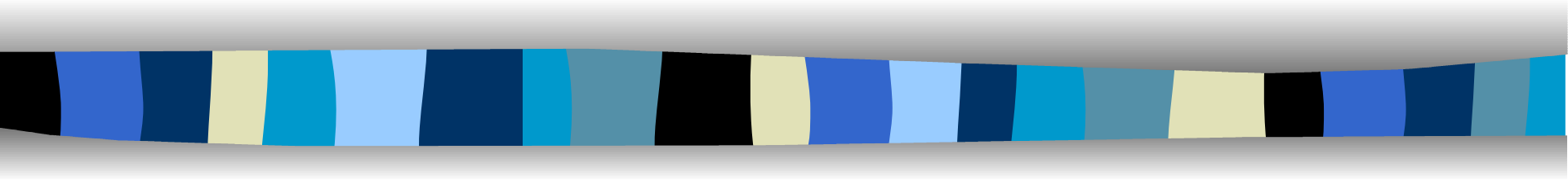
Større sikkerhetsrissiko

# Introduksjon

“Forstår man ikke teknologien, får man et feil bilde av rissikoen ved å benytte den…”

“De fleste brukere er fornyød så lenge det ser ut til å fungere…”

# Ulike teknikker



# Ulike teknikker

- Manipulere e-post
- Manipulere websider
- Phishing
- Pakkesniffing

# Manipulere e-post

- Svært få har en anelse om hvor enkelt det er å generere epost "manuelt"
- Kan delvis gjøres gjennom mailklient, men best gjennom telnet
  - *Eksempel: Mail fra Kaptein Sabeltann*

# Mottiltak

- Signering av mail
- Verifiser innhold med avsender
- Sjekk mistenkelig mail
  - Kan finnes spor i «replay-to» feltet
  - Har annet innhold/ordlyd enn man skulle forvente

# Manipulere websider

- Folk har en tendens til å stole på det som står skrevet…
- Enkelt å endre uten å endre selve websidene på serveren
  - Parametere
    - Eksempel: google, sa-vær
  - Brukergenerert data
    - Eksempel: gjestebok, nettavis
  - Lokal versjon
    - Eksempel: nettavis (fil/firebug)
  - Skjemadata
    - Eksempel: matbestilling

# Mail fra Posten Norge AS - tollavdeling

*"Jeg gjør oppmerksom på at mail ikke er godt nok som dokumentasjon på at avsender/eksportør har gitt feil informasjon. (Verken utskrift av mail, videresendt mail, mail i vedlegg). Som dokumentasjon kan brukes: faktura, ordrebekreftelse (paypal/e-bay), den siste siden fra nettet, som viser det fullstendige kjøpet som er fullført (med alle opplysninger om kjøpet/sendingen). "*

# Mottiltak

- Vær kritisk til url'er man mottar:
  - sjekk parametere
- Vær kritisk til websider
  - som er lagret lokalt
  - utskrift
  - som inneholder brukerdata
- Generelt: Vær kritisk til informasjon på nettet

# Phishing

- Lage en kopi (dynamisk) av en kjent webside
- Flere bruksområder:
  - Gi uriktig informasjon
    - Eksempel: vgnetproxy
  - Stjele informasjon
    - Eksempel: loginphishing

# Mottiltak

- Kontroller alltid domene
  - Også: http://www.vg.no@tomheine.net
- Vær obs på redirects
- Vær obs på frames
- Installer Phishingfilter
  - Eksmepel: Username-url i firefox 3.0

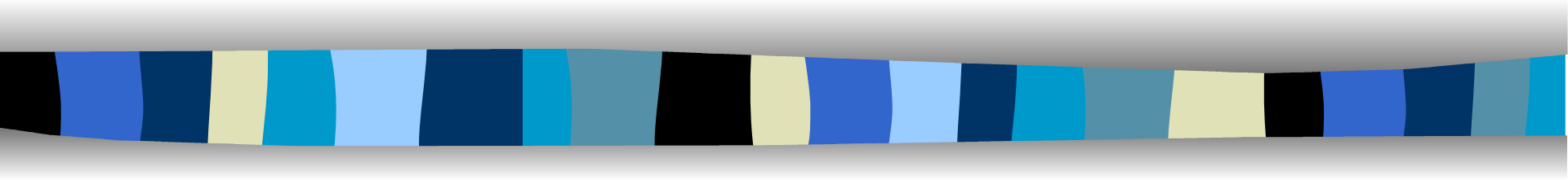
# Pakkesniffing

- Gir tilgang til all datatrafikk
- To interesseområder/farer
  - Hvilke data blir sendt (klartekst)
  - Når/hvor mye data blir sendt (klartekst/kryptert)
- Kan kobles til hvor som helst i nettet
  - Eksempel: WireShark

# Mottiltak

- Send aldri viktig informasjon gjennom åpne kanaler/tjenester
- Tenk gjennom hvor du befinner deg/er koblet til
  - Spesielt trådløse ”ekstrastasjoner”

# Social Engineering



# Social Engineering

- Før var det tekniske løsninger som stod for trusslene, nå er det gjennomtenkte ideer
  - Eksempel: “Ringe fra Helpdesk”
- Forsøker (til en viss grad) å gå mot enkeltindivider istedenfor massene
- Ofte via mail

**Subject:** **Unauthorized Access to your account.**
**From:** service@intl.paypal.com
**Reply-To:** akstcamwayvebsomnsdqs@amwayvebso.ru
**Date:** 26.04.2008 21:56
**To:** ost@tomheine.net

PayPal

We recently reviewed your account, and we need more information about your business to allow us to provide uninterrupted service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible. We apologize for the inconvenience.

---

**Why is my account access limited?**

Your account access has been limited for the following reason(s):

- We have reason to believe that your account was accessed by a third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive PayPal account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

(Your case ID for this reason is PP-136-124-102.)

---

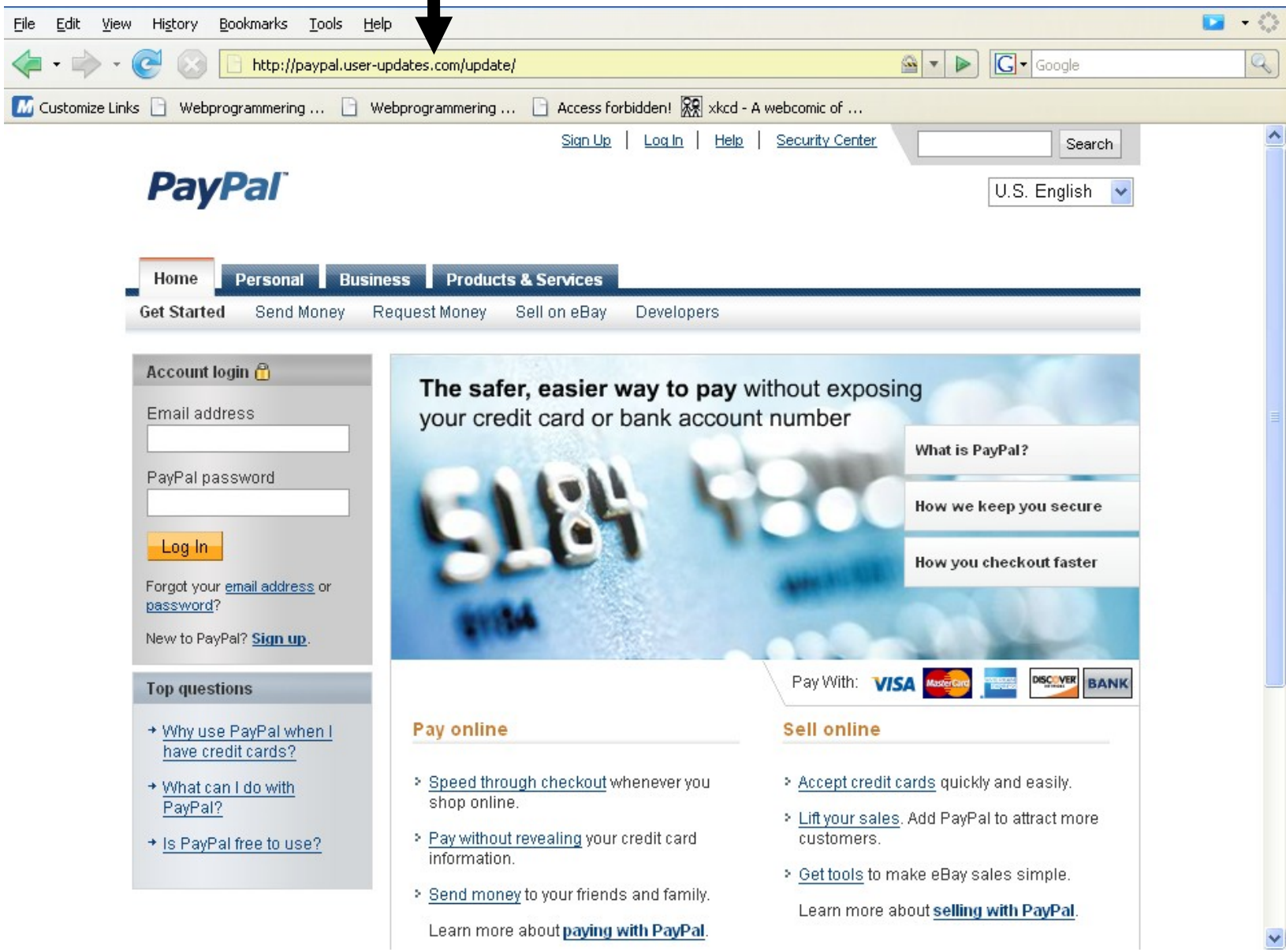
**How can I restore my account access?**

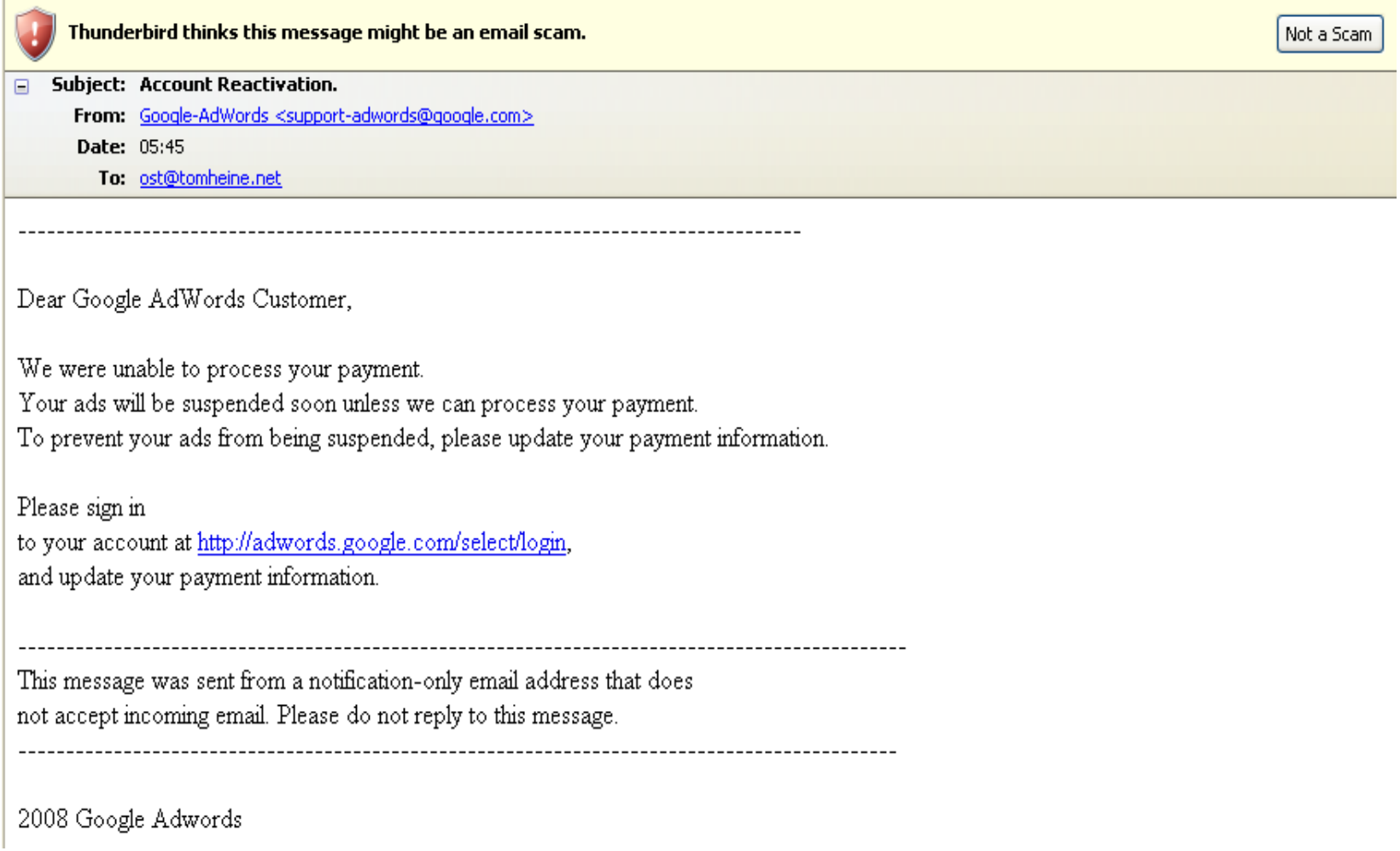
Please visit the **Resolution Center** and complete the "Steps to Remove Limitations."

**Completing all of the checklist items will automatically restore your account access.**

---

# http://paypal.user-updates.com/update/





Thunderbird thinks this message might be an email scam.

Not a Scam

**Subject:** **Account Reactivation.**
**From:** Google-AdWords <support-adwords@google.com>
**Date:** 05:45
**To:** ost@tomheine.net

---

Dear Google AdWords Customer,

We were unable to process your payment.
Your ads will be suspended soon unless we can process your payment.
To prevent your ads from being suspended, please update your payment information.

Please sign in
to your account at http://adwords.google.com/select/login,
and update your payment information.

---

This message was sent from a notification-only email address that does
not accept incoming email. Please do not reply to this message.

---

2008 Google Adwords

**http://www.adwords.google.com.ks7hd.cn/select/Login**

# Hvorfor virker dette?

- Sender til et stort antall
- Folk flest er redde for å miste konto/penger
- Få vet om at man kan sende mail fra hvilken som helst e-mailadresse
- Folk flest tror ikke at noen gidder gjøre en bløff så "bra"
    - Bygget opp på samme måte som f.eks PayPal sine systemmail (checklist osv)
- F.eks PayPal er for mange synonymt med "trygghet"
- Folk flest har liten forståelse for URL'er

# Hvordan forhindre?

- Gå aldri inn på websider via linker i mail
- Vær forsiktig med å laste bilder i mail
- Se etter personlig informasjon
- Kontakt organisasjonen som “har sendt” ut mailen og bekreft
- Ikke svar / meld deg av SPAM
- Benytt en spesiell mailadresse til viktige tjenester

# Digitalt fotavtrykk

# Digitalt fotavtrykk

- Det meste vi gjør på nettet legger igjen spor
  - Vår maskin
  - Internetleverandøren
  - Transportledd
  - **Benyttete ressurser (websider, mail osv)**
  - **Indekserende ressurser (google)**

# Digitalt fotavtrykk: Eksempler

- Det vi har lagt på nettet, blir ikke borte
  - Google cache
  - http://www.archive.org/web/web.php
- Autokorrektur i MS Word
  - Eksempel: Mehlis-report

# Digitalt fotavtrykk
## – Forhåndsregler

- Aldri legg ut ting du ikke vil skal være tilgjengelig for all fremtid
  - F.eks mhp fremtidige arbeidsgivere
- Tenk på hvordan du legger ut informasjon
  - F.eks tom.h.natt@hiof.no vs tom.h.natt (at) hiof.no
- Ikke stol på at «ingen har URLen»
  - Eksempel: CNN sin episode med nekrologer
- Google deg selv fra tid til annen
- Vær spesielt forsiktig med sosiale nettverk
  - Personlig informasjon satt i system…
- Husk at også det du gjør på nettet logges i stor skala

# Identitetstyveri

# Identitetstyveri

- Kun en liten del av dette er å benytte kredittkortnummer
  - Opprette abbonementer og kontoer i andres navn
  - Poste innlegg, sende mail osv
  - Overta kontoer (spes. Sosiale nettverk osv.)
  - Utføre illegale handlinger
- For mye informasjon er samlet i tilgjengelig og linkbare registere
- Merker det ikke
  - “Ingen lommebok som blir stjålet”

# Identitetstyverier
## - Eksempler

- Tele 2 – saken
- MSN-block-list
- Canadiske pass-historien

# Identitetstyveri
## – Hvordan forhindre

- Ha flere sett med passord til ulike "nivåer" av tjenester
- Oppgi aldri brukernavn/passord til "krysstjenester"
- Begrense (så mye som mulig) av offentlig informasjon på websider osv…
  - Nettkataloger, registere osv.
- MAO: Begrense det digitale fotavtrykket

# Oppsummering

# Oppsummering

«Det er en viktig balansegang mellom nettsikkerhet og å bli paranoid»

«Det er ofte det minst mistenkelige som er farligst»

«Som oftest er teknologien sikker, men er det alltid noen som finner en måte å utnytte den slik at det blir en sikkerhetsrisiko for andre»