RESEBYRÅBEDRÄGERIER
ERFARENHETSUTBYTE

JOHANES HASSMUND
LIU IRT

Update Webmail

Linköping University email system and calendar services services have been updated.

Visit the updated Outlook Web App http//owa.liu.se/ for information and instructions on how to access your email.

Accessing your mail through the web: http//owa.liu.se/

Linköpings universitet e-postsystem och kalendertjänsterservices har uppdaterats.

Besök den uppdaterade LIU Outlook Web App på http//owa.liu.se/ för information och instruktioner om hur du kommer åt din e-post.

Komma åt din mail via webben: http//owa.liu.se/

- Updated Webmail includes a refreshed interface with abs on top and a new inbox email default theme.
- Beginning on Wednesday, Dec 03rd 2014, the new web-mail application becomes the default for all users.
- Updated to improve performance (Standard and Basic interfaces)

Tidslinje

Tidpunkt	Händelse
T-7d	Nytt resebyråavtal i drift Återställningslänk för lösenord skickas till samtliga användare
T	Nätfiskebrev till en begränsad grupp användare
T+1d	Två användare går på bedrägeriet
T+3d	Återställningslänk skickas för att komma åt bokningsportalen
T+5d	Bedrägeriet upptäcks av resebyrån Oanvända biljetter avbokas – om det går (!) Self-service portal stängs för LiU
T+21	Förbättrat nätfiskebrev till ca 4000 användare; ingen gick på det (vad vi vet)

Sårbarheten

Vi är sårbara mot phishing (surprise)

Självserviceportelen tillåter bara att du bokar åt dig själv, men…

- Du kan byta namn. Hur många gånger du vill! **←WTF?**
- Inga kontroller av att namnbytena är rimliga.

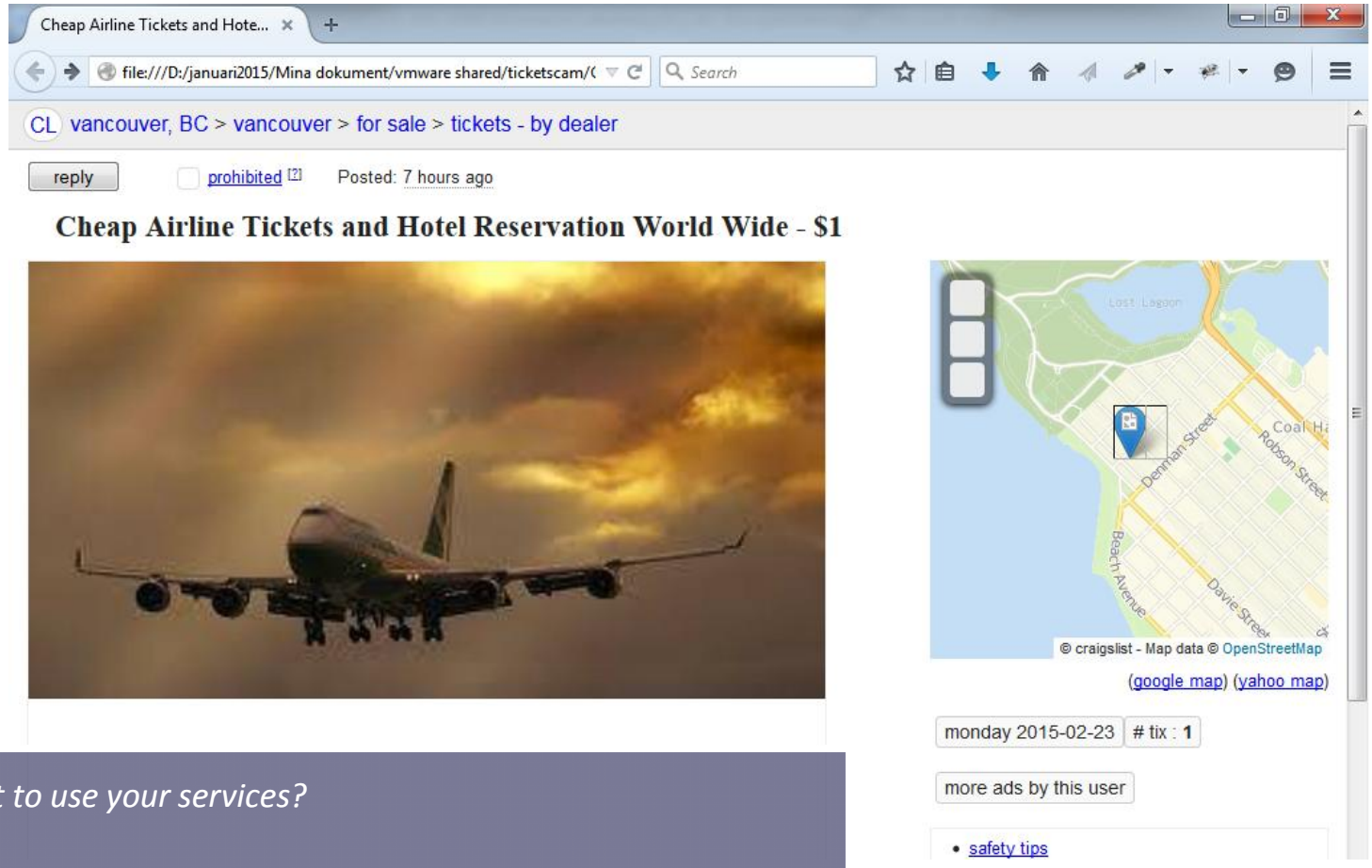
African connection

- Anslutande IP-adresser tillhör sydafrikansk ISP.
- Nästan alla passagerare har afrikanskklingande namn.

38 flights could not be canceled. The majority involve African airports or have connecting flights to Africa.

Linköpings universitet

Gör din egen resebyrå



Q: How safe is it to use your services?

A: We can put it this way, when you book with us, it will be the closest you come to booking legally. There will never be any problem. With us, you can be guaranteed you pay for quality, with your safety as priority.

Attacken

Phishingbrevet saknade de vanligaste kännetecknen

- Inga hot, hyffsat språk, trovärdigt
- Uppföljningsbrevet ännu bättre (med vår footer)

Phishingsiten identisk med den riktiga

- Vid misslyckad inloggning blev man omdirigerad till den äkta siten (det vill säga inloggning funkar på andra försöket).

Falska länkar svåra att upptäcka

- OWA skriver om länkar

E-postkonton konfigurerades att dölja aktiviteten

Slutligen lite gnäll

- LiU var nummer fem (!) att drabbas av bedrägeriet men det första lärosätet som varande andra och informerade CERT-SE.

- Om det nu är så att man undviker att informera för att det är pinsamt. Använd Sunet CERT som proxy!

Linköpings universitet

www.liu.se