SRU

PRACTICAL TIPS TO STAY TECHSAFE

Please login to a computer and go SRU Homepage:

www.sru.edu

Keyword: TechSafe

PHISHING & SUSPICIOUS EMAIL

How good are you at catching a Phish?

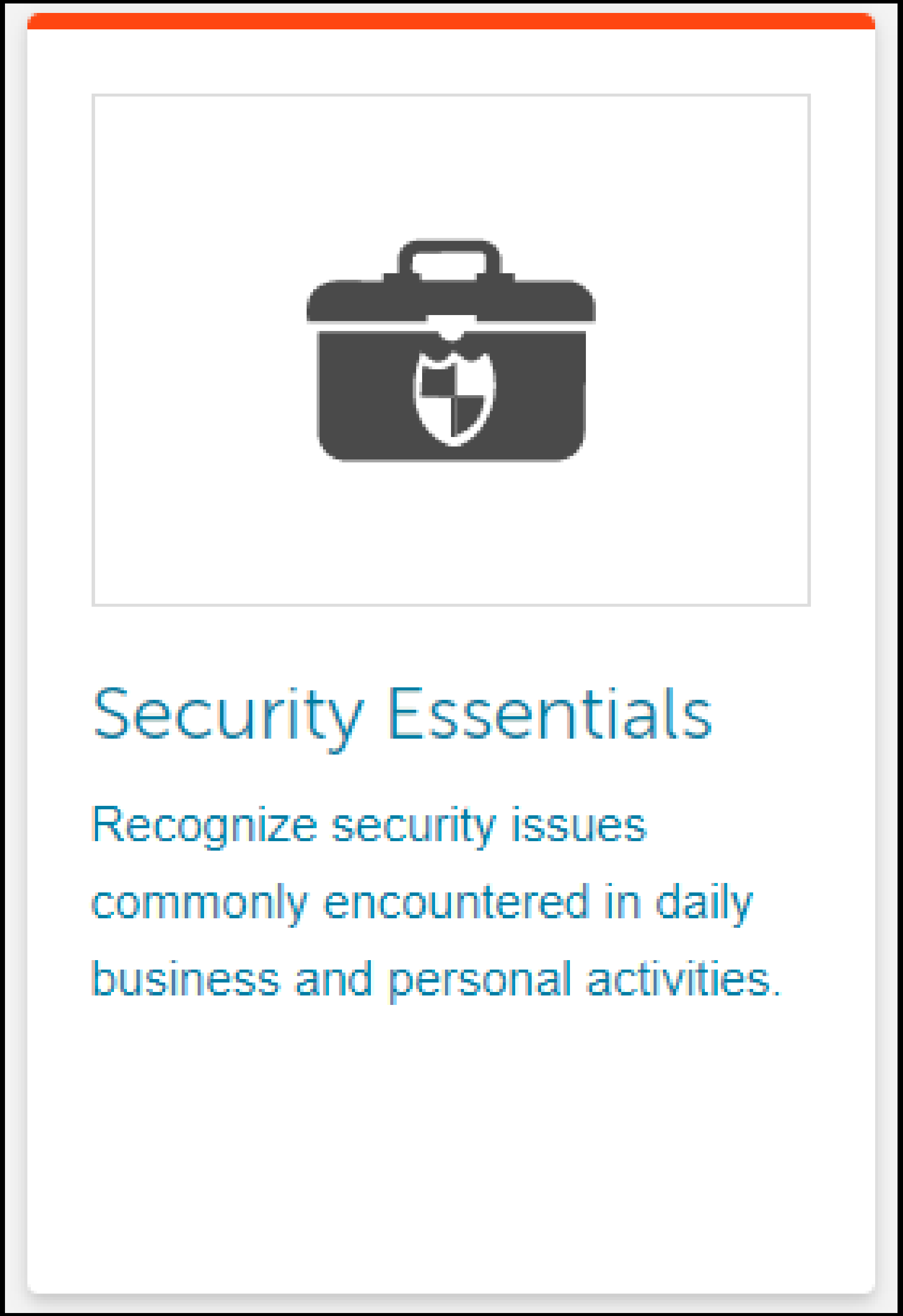
Take this Phishing Quiz

PRACTICAL TIPS TO STAY TECHSAFE

Please login to a computer and go to the following site:

sru.securityeducation.com

Wombat



Security Essentials

Recognize security issues commonly encountered in daily business and personal activities.

CYBERSECURITY SESSIONS

BRODY MCKENNA

IATS – SUPPORT SERVICES STUDENT TECHNICIAN

ABOUT ME

- Management Information Systems Major
- Cybersecurity Minor
- 2 years with IATS

EMAIL SECURITY

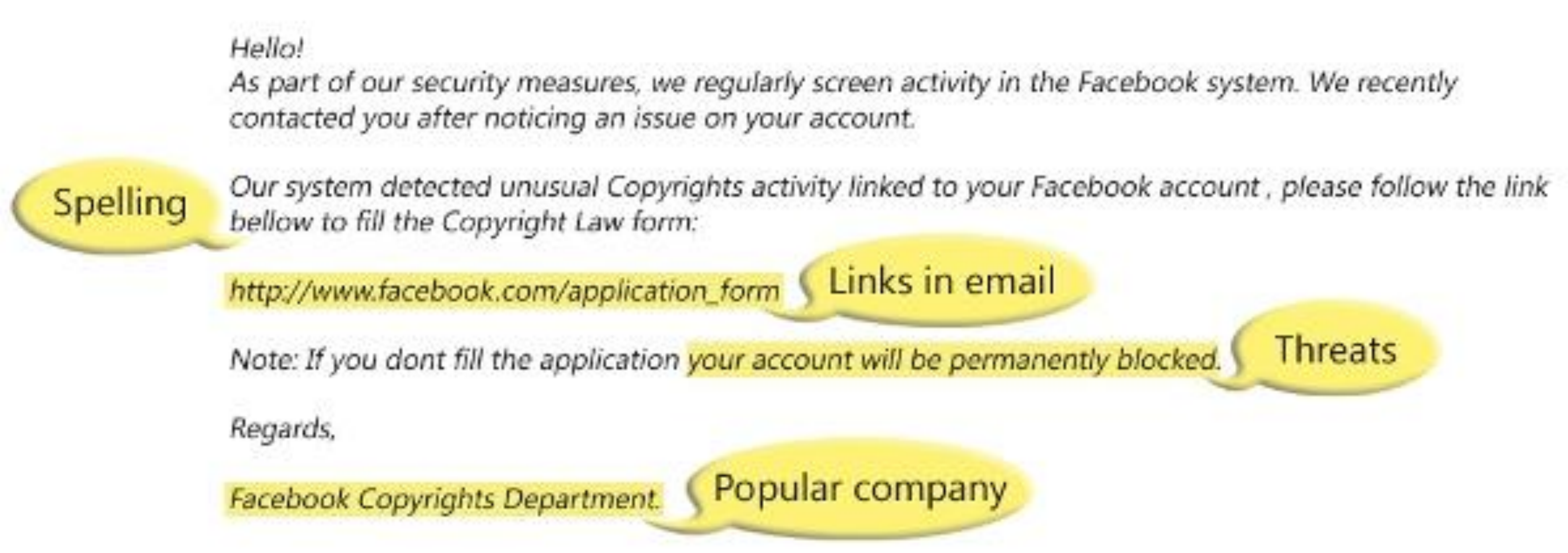
WHAT IS PHISHING?

- An online attempt to gain information
- Pretend to be legitimate, and trustworthy
- Examples of stolen information:
  - Login information, credit card/bank numbers, money

- The volume of spam mail has increased 4x since 2016.

HOW TO SPOT THEM

- The use of urgent language
- Bad grammar and spelling
- May ask you to validate/update credentials
- Ask for personal information, bank info, and/or credit card numbers
- Hover over links to see the real website address



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

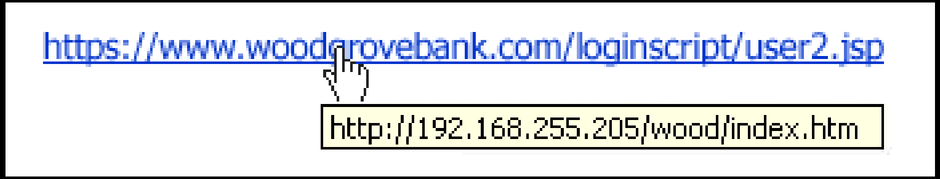
Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

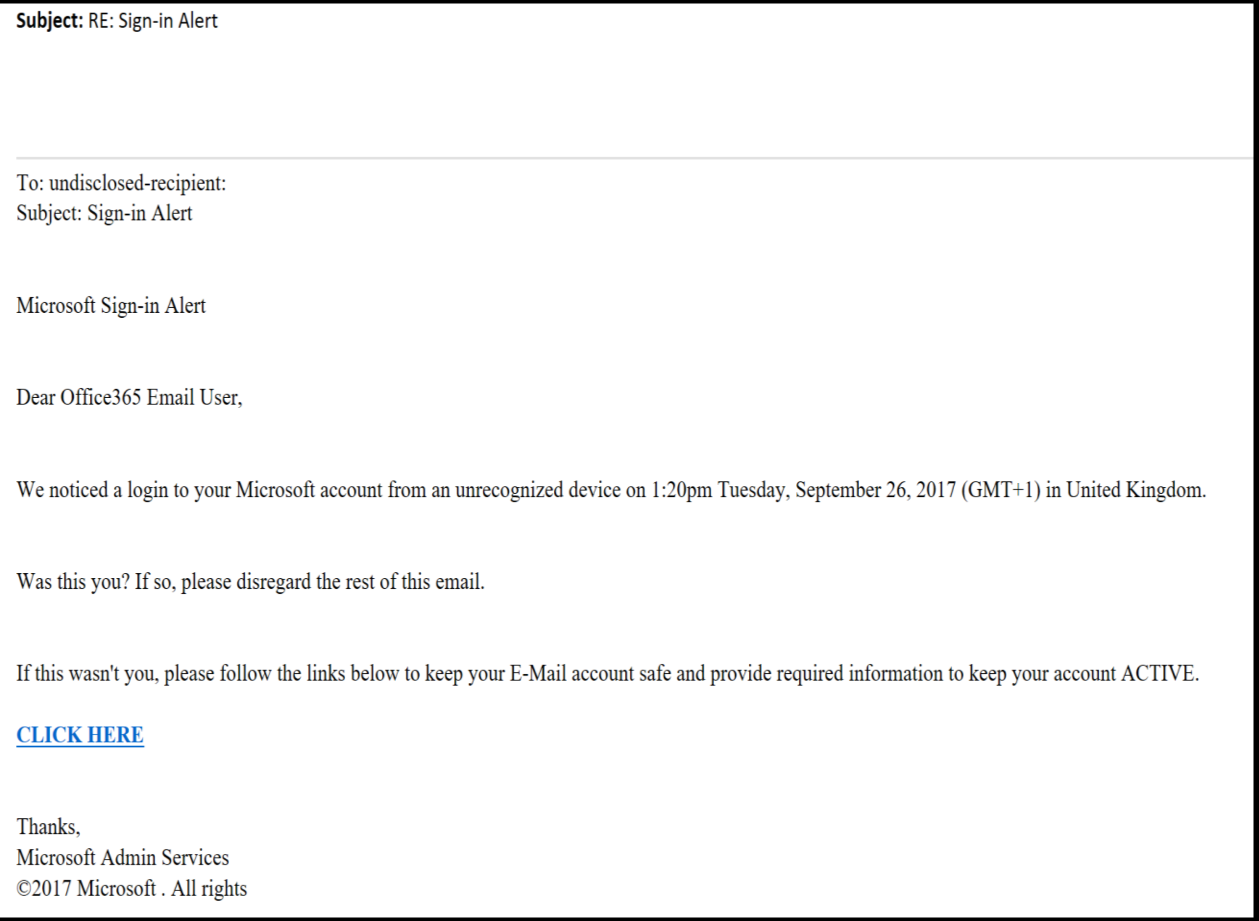
Facebook Copyrights Department.



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

Microsoft.com



Subject: RE: Sign-in Alert

To: undisclosed-recipient:
Subject: Sign-in Alert

Microsoft Sign-in Alert

Dear Office365 Email User,

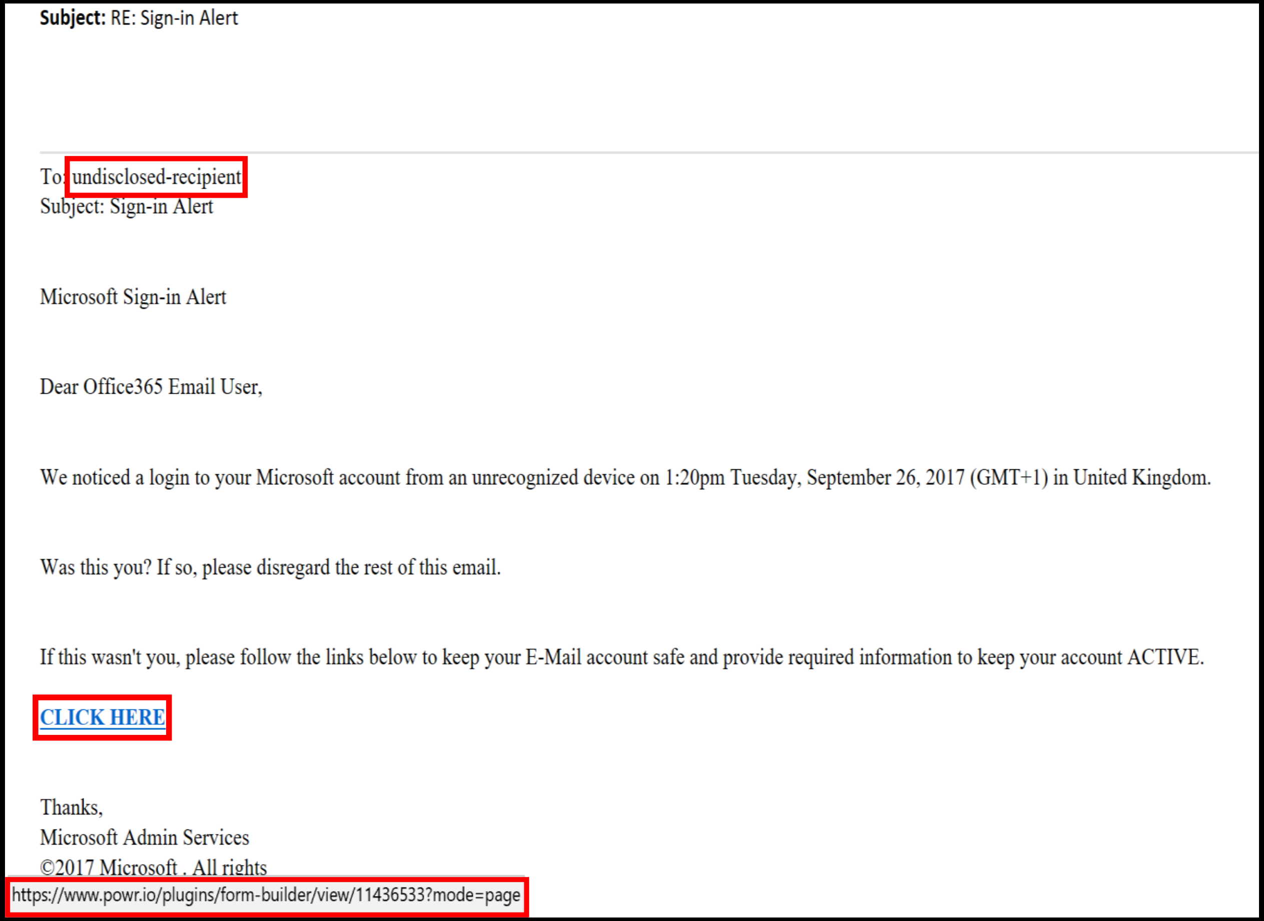
We noticed a login to your Microsoft account from an unrecognized device on 1:20pm Tuesday, September 26, 2017 (GMT+1) in United Kingdom.

Was this you? If so, please disregard the rest of this email.

If this wasn't you, please follow the links below to keep your E-Mail account safe and provide required information to keep your account ACTIVE.

CLICK HERE

Thanks,
Microsoft Admin Services
©2017 Microsoft . All rights



Subject: RE: Sign-in Alert

To: undisclosed-recipient
Subject: Sign-in Alert

Microsoft Sign-in Alert

Dear Office365 Email User,

We noticed a login to your Microsoft account from an unrecognized device on 1:20pm Tuesday, September 26, 2017 (GMT+1) in United Kingdom.

Was this you? If so, please disregard the rest of this email.

If this wasn't you, please follow the links below to keep your E-Mail account safe and provide required information to keep your account ACTIVE.

CLICK HERE

Thanks,
Microsoft Admin Services
©2017 Microsoft . All rights

https://www.powr.io/plugins/form-builder/view/11436533?mode=page

SRU FRAUD EMAILS

- Directs you to a non-SRU website
- Asks you to validate account information or risk deactivation
- The sender’s address is fake
- Fake Logos, bad grammar, etc

- If you suspect Phishing, contact the help desk

IF YOU DO CLICK THE LINK

- Your account could be compromised
    - Change your important passwords immediately
    - Report the issue
- Configure your SRU Maintenance Tool to manage your account password

PHISHING GAME

- In your browser go to sonicwall.com
- In the search type Phishing
- Select Phishing IQ Test

TAKEAWAYS

- Use caution with risky looking computers
- Be suspicious of emails requesting personal info
- Verify legitimacy
- Set up your SRU Maintenance tool to reset and manage password.

MOBILE PHONE SECURITY

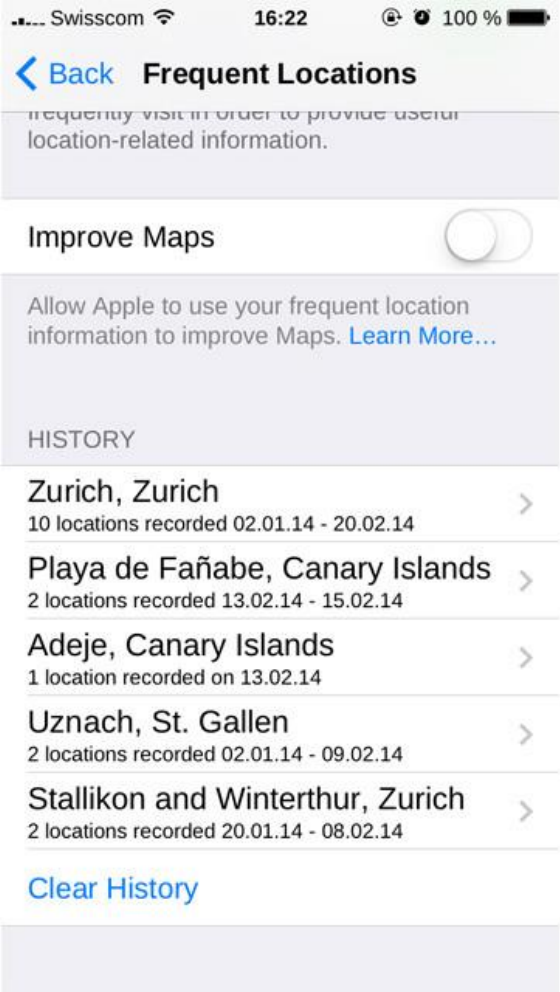
SECURING YOUR DEVICE

- iPhone
  - 4-digit passcode, 6-digit passcode, alphanumeric password, Touch ID, Face ID
- Android
  - PIN, password, slide, swipe pattern, Face (picture) unlock

LOCATION SERVICES

- iPhone and Android both constantly track and store frequent locations

IPHONE LOCATION TRACKING



< Back **Frequent Locations**

frequently visit in order to provide useful location-related information.

Improve Maps ○

Allow Apple to use your frequent location information to improve Maps. Learn More…

HISTORY

Zurich, Zurich
10 locations recorded 02.01.14 - 20.02.14

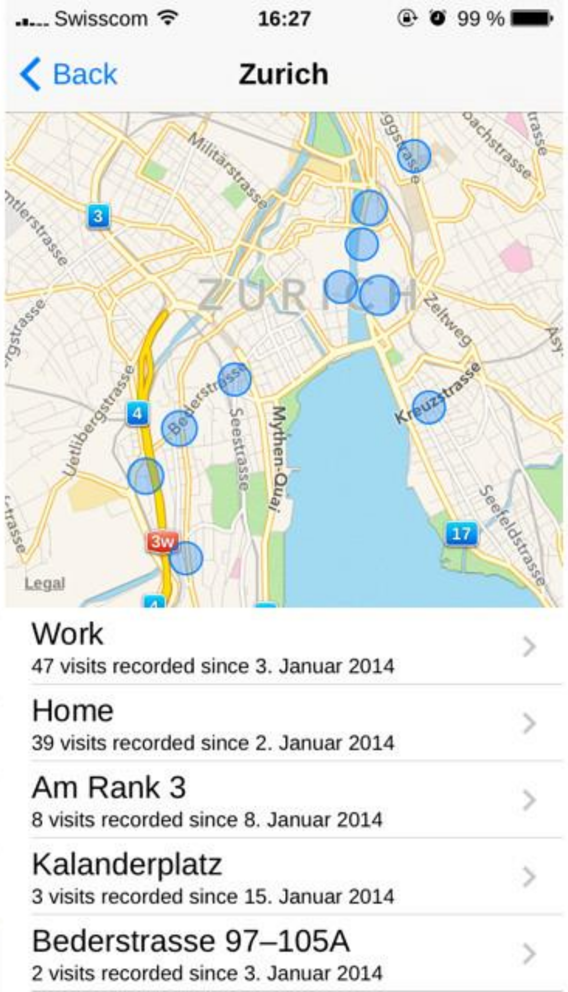
Playa de Fañabe, Canary Islands
2 locations recorded 13.02.14 - 15.02.14

Adeje, Canary Islands
1 location recorded on 13.02.14

Uznach, St. Gallen
2 locations recorded 02.01.14 - 09.02.14

Stallikon and Winterthur, Zurich
2 locations recorded 20.01.14 - 08.02.14

Clear History



< Back **Zurich**

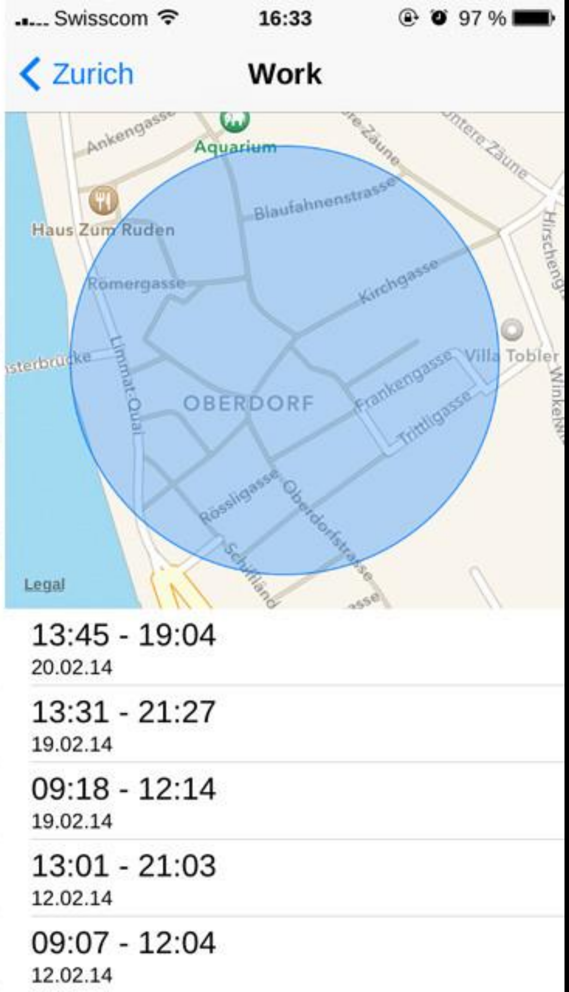
Work
47 visits recorded since 3. Januar 2014

Home
39 visits recorded since 2. Januar 2014

Am Rank 3
8 visits recorded since 8. Januar 2014

Kalanderplatz
3 visits recorded since 15. Januar 2014

Bederstrasse 97–105A
2 visits recorded since 3. Januar 2014



< Zurich **Work**

13:45 - 19:04
20.02.14

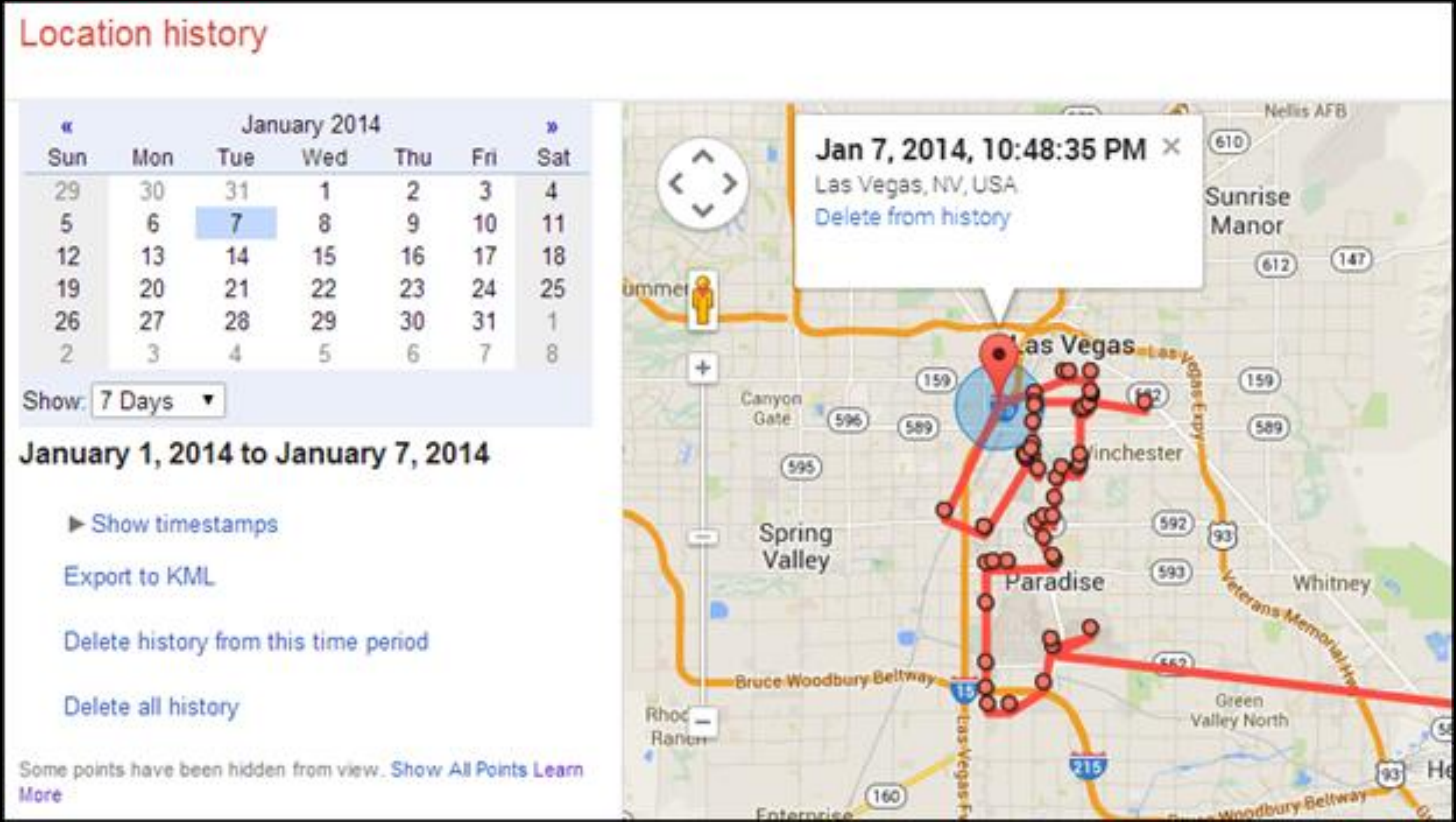
13:31 - 21:27
19.02.14

09:18 - 12:14
19.02.14

13:01 - 21:03
12.02.14

09:07 - 12:04
12.02.14

ANDROID LOCATION TRACKING



Location history

« January 2014 »

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Show: 7 Days ▾

January 1, 2014 to January 7, 2014

▶ Show timestamps

Export to KML

Delete history from this time period

Delete all history

Some points have been hidden from view. Show All Points Learn More

Jan 7, 2014, 10:48:35 PM ×

Las Vegas, NV, USA

Delete from history

HOW TO STAY SAFE

- Download content from safe places
- Back up your data
- Keep your phone and apps on the most recent update
- Turn off Wi-Fi and Bluetooth when not in use
  - Also saves battery
- Beware of phishing texts
- Have locating service activated if you lose your phone
  - Can be used to locate, lock, or wipe your phone remotely
- Be mindful of the permissions you grant to apps

SAFE BROWSING TIPS

BASIC TIPS

- Use Privacy settings
- Do not make personal information public
  - Keep it limited and professional
- Be careful of downloading anything
- Use strong passwords or pass phrases
- Only make payments through secure sites
- Be mindful of what you post and whom you meet
- Keep antivirus up-to-date

As tempting as the free cruise might sound, DO NOT click the link!

Resources:

https://www.sru.edu/offices/iats/techsafe