Module 4

Don't Skip Me - Countermeasures

1. Secure your account:

   ✓ Enable Step 2 / one time password Authentication, so even if the attacker got your username/password he still needs to have the one time password and he has to use before you! Because once the legitimate user enters the one time password it becomes invalid immediately.

   - Gmail provides SMS and Gmail mobile app
     https://www.google.com/landing/2step/
     https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en

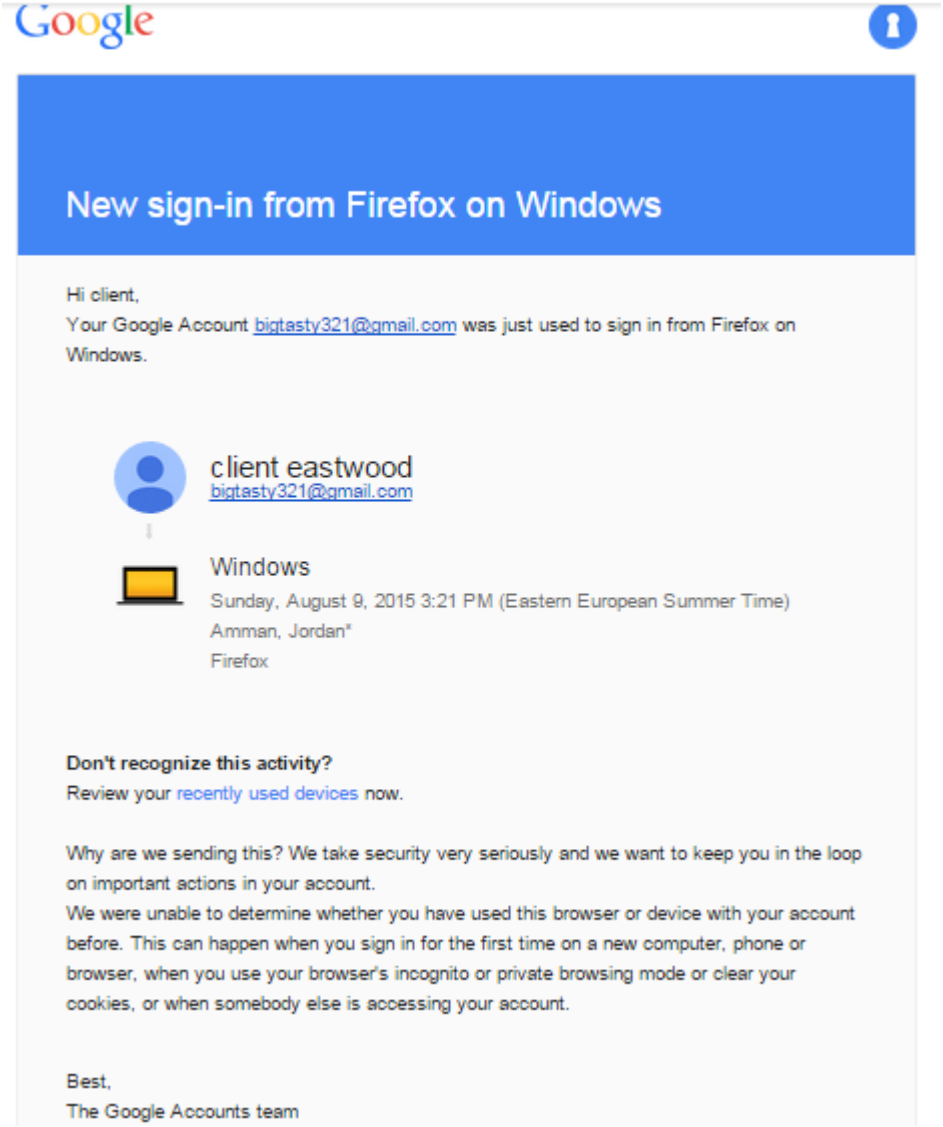
   - Paypal provides mobile app and Email
     https://www.paypal.com/webapps/mpp/security/online-security-guide

   - Facebook provides many methods
     https://www.facebook.com/help/413023562082171

- Twitter provides mobile app and SMS https://support.twitter.com/articles/20170388

[!] Note: - You may still vulnerable to session hijacking attack but the chances for a successful attack much less.

✓ Pay attention to new sign-in notification, like this one



Google

New sign-in from Firefox on Windows

Hi client,
Your Google Account bigtasty321@gmail.com was just used to sign in from Firefox on Windows.

client eastwood
bigtasty321@gmail.com

Windows
Sunday, August 9, 2015 3:21 PM (Eastern European Summer Time)
Amman, Jordan*
Firefox

Don't recognize this activity?
Review your recently used devices now.

Why are we sending this? We take security very seriously and we want to keep you in the loop on important actions in your account.
We were unable to determine whether you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer, phone or browser, when you use your browser's incognito or private browsing mode or clear your cookies, or when somebody else is accessing your account.

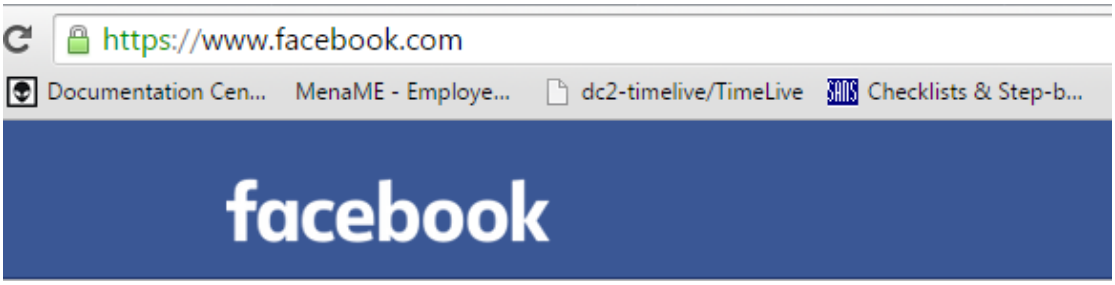
Best,
The Google Accounts team

- ✓ Use strong and complex password – no more "123loveyou" – please!

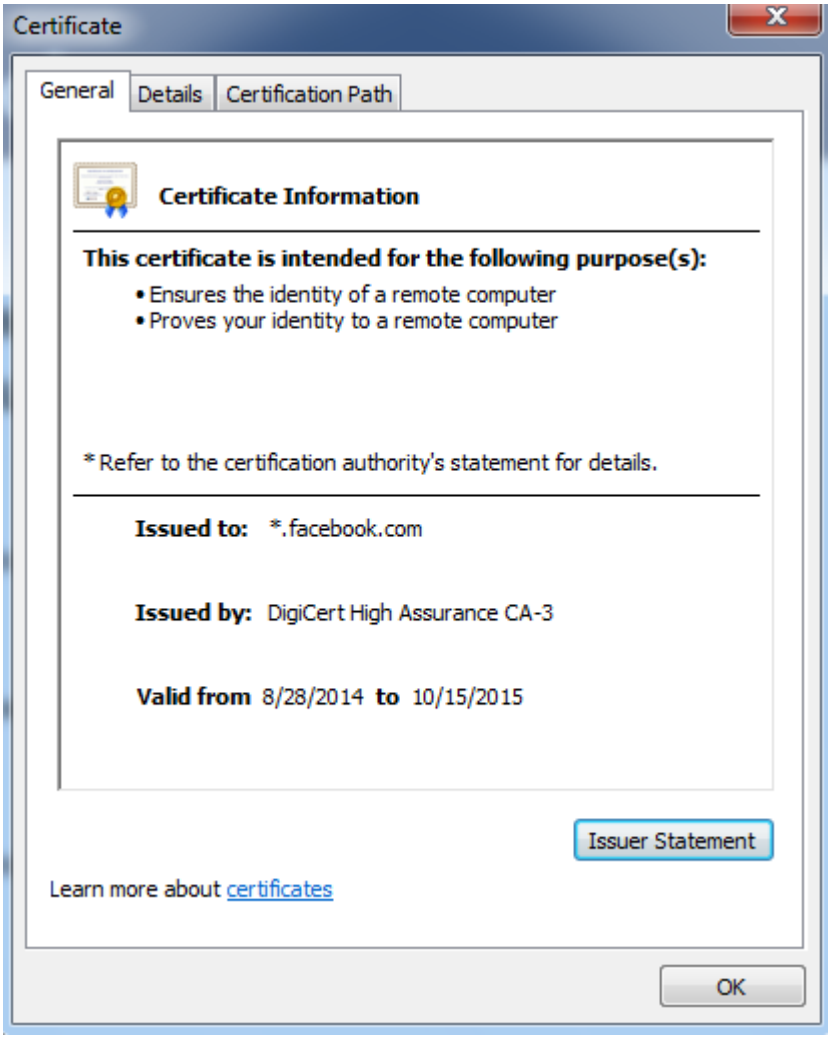
2. Secure your computer :
   - ✓ Use non admin account – always!
   - ✓ Keep your browser and system updated
   - ✓ Consider the previous countermeasures, especially in module 2

3. Secure your network : we didn't cover network based attacks however if you plugged into un-trusted network like a wifi in café, then consider to use VPN as it will protect all you data in transit.

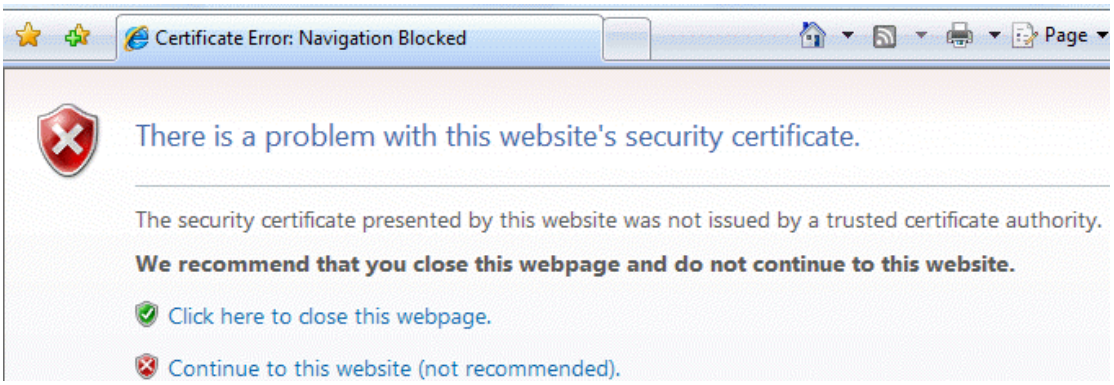
4. Open your eyes on any suspicious activity such as
   - ✓ Missing https from the login URL

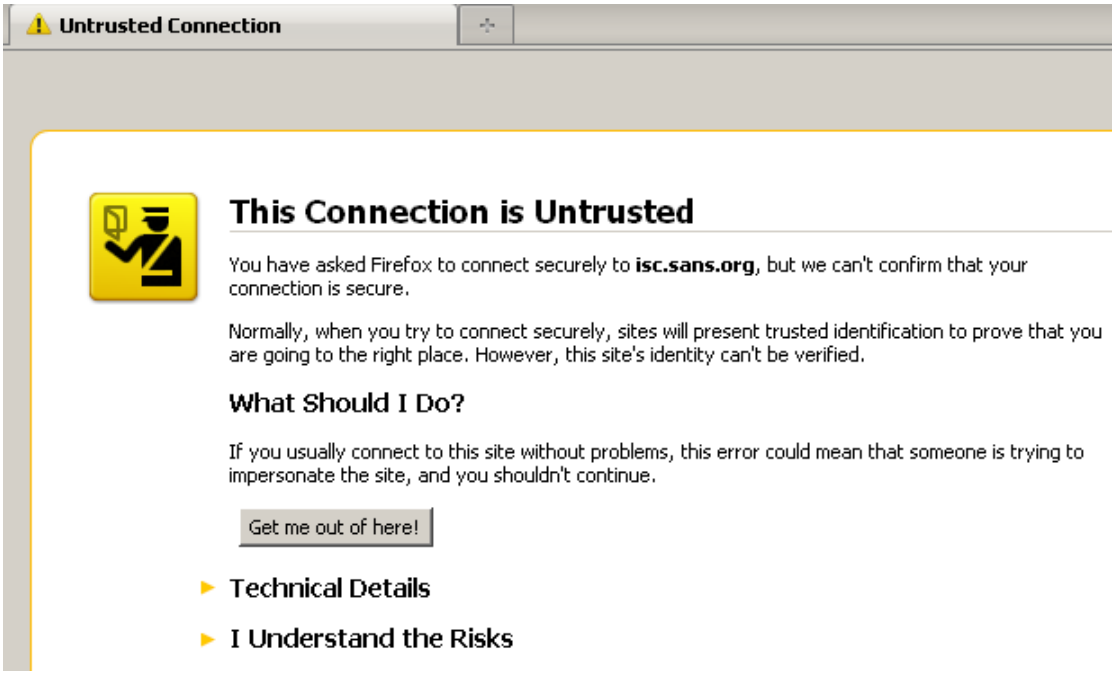


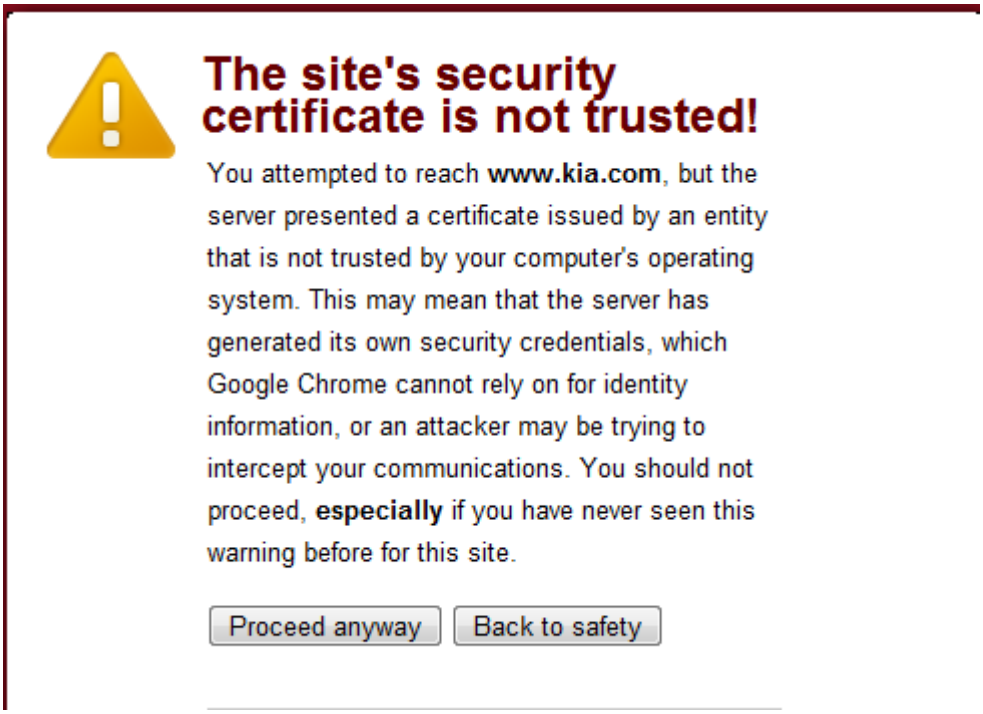
Do an extra mile and verify the SSL/TLS certificate information and certification path.



✓ SSL/TLS Certificate error







- ✓ Banks will never ask you to provide your password via email – this is likely a phishing email. https://www.paypal.com/us/webapps/helpcenter/helphub/article/?solutionId=FAQ2331