… Created by Mike Bloomfield

'Internet Security - Ecommerce'

July 2004

Internet Banking and Internet Shopping Basic

1. Use a current version browser.

- Use your browser's built-in security features provided. Choosing certain security settings and options will help protect the privacy of your accounts and personal information.

  http://www.microsoft.com/security/incident/settings.mspx
  http://www.microsoft.com/windows/ie/using/howto/security/settings.mspx

- Always update your browser when new versions are released. They often include new security features.

- Check your browser for built in safety features that you may or may not elect to use.

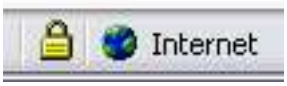
2. Do you know them?

- Is the receiver somebody you can trust?

- Buying books from “Amazon.com” is okay, but would you send your credit card details to “fakeamazon.com”?

3. Make sure your data is encrypted.

- When you send sensitive information, like passwords or credit card details. Make sure there is a “lock” on your browser, which means your information will be sent with S.S.L. (Secure Socket Layer) encryption.



-

Copyright APCGENIUS 2004

4. Protect the confidentiality of your User ID and Password.

- Make your password unique to you and change it regularly. You should never use a password that would be easy for others who know you to guess, or one that a common password cracking utility could find.
- Memorize your password. Your online password authenticates you when you begin an online Banking session. You should memorize this password and never write it down anywhere or reveal it to anyone. Sharing your password or PIN with another is the same as giving that individual authority to use your name in a transaction.
- Do not say your password out loud.

5. Log off when you are finished

Internet Transactions are Safer Now…

Now, we are more confident to send financial information over Internet.

Okay, try to convince me to use Internet banking:

1. Most Banks Guarantee that you will not be liable for any unauthorised transactions that may be carried out on your credit cards and bank accounts.

2. Using Credit Cards over the Internet is safer than using a credit card in a local restaurant.

   - When you send credit card information to a trustable online store, your credit card details will be encrypted with 128bit S.S.L. encryption.
   - When you use your credit card in your daily life, everyone can read all the information on your card.

3. I feel safer sitting in front of my computer to do Internet Banking rather than do banking in front of the ATM at night.

Copyright APCGENIUS 2004

Or is it…
http://www.hkab.org.hk/PDF/customer_info/ebanking_e.pdf
http://www.exposures.co.nz/modules.php?name=News&file=article&sid=278
http://www.tinhat.com/banking/online_banking.html

Protect yourself

The weak points in internet bank security are you and your computer. Which means you should take some steps to protect yourself:

- **Get a decent password and change it every two months. In a recent study of bank security, some 40% of respondents used the word 'password' as their password. If you fall into that group, stop being so silly.**
- **Make sure that your bank's site is encrypted before you enter any personal details. You can check that a site is encrypted by looking at the address. If the address starts with https (rather than http) then you are safe.**
- **Install a reputable anti-virus programme on your computer to protect yourself against viruses that record the keys you press (logger viruses), giving hackers the ability to see what you are doing in your computer.**
- **Make sure your browser is the latest version. Free updates are available for both Window's Explorer and Nestcape, the two most popular browsers, from their websites. The latest versions are safer than the earlier ones.**
- **Avoid using internet cafes to access your online bank. Computers in these cafes are more likely to have viruses that will give away your password. There's also a chance that the next person to use the computer might stumble across details you have unwittingly left there.**
- **Don't give any banking details out using email. Email's are not secure and are relatively easy to snoop on. It's highly unlikely your bank will ask you for any information by email - be very suspicious of any such contact.**
- **Be wary of the growing scam called 'phishing' or 'spoofing'. This is where crooks set up fake banking sites then send emails to people to get them to visit the site and give away their details. If you have any doubts then contact your bank directly and ask them to verify an email you have received.**

"Is Internet Banking Safe", Channel 4, U.K.

The Internet is a transmission tool; this topic discusses transmission protection. The matters after the transmission like how will the receiver handle the information, credit card processing, etc. is out of the scope of this topic.

Kind Regards,

Mike Bloomfield

Copyright APCGENIUS 2004