Being Connected *and* Secure: Lessons for Everyday Computer Use

By Dr. Roozmehr Safi

Presented at

SenCom

UMKC

UNIVERSITY OF MISSOURI-KANSAS CITY

Agenda

- Why does security matter?
- Who should be concerned?
- Major types of security threats
- General security advice
- Q&A

Introduction

- **Q:** Why is security important?
- **A:** For various reasons:
  - Identity Theft
  - Monetary Theft
  - Privacy issues
  - Legal Ramifications

- Today's hackers are career criminals
- Online fraud is now a global industry
  - Hacking tools being bought and sold easily
  - Markets exist for stolen goods (credit card numbers…)
  - Virtual money for payments (bitcoin…)

Introduction, Continued

Q: Who should be concerned about information security?

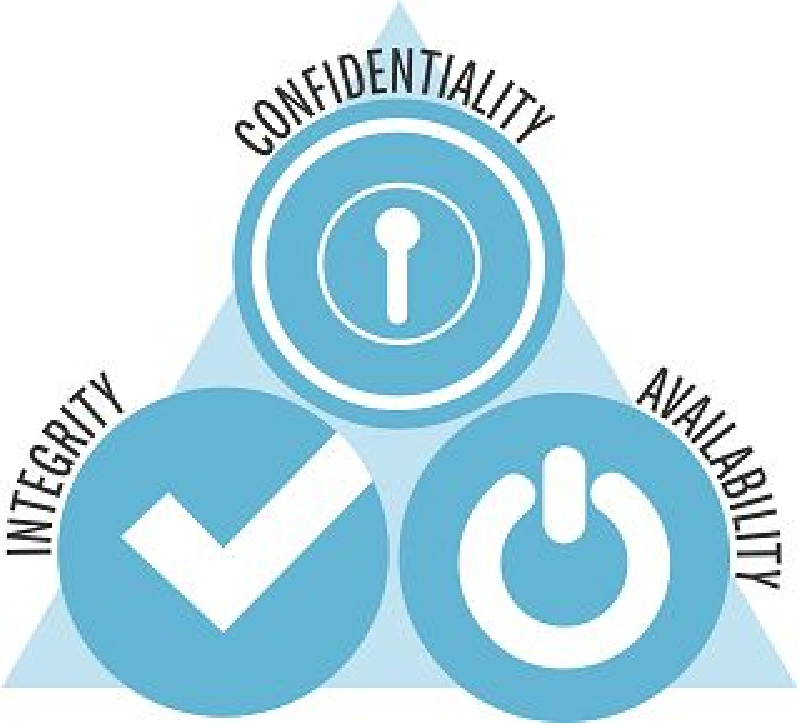
A: Anyone who uses:

- Computers
- The Internet
- Email
- Smart phones
- Social Networks…

Keeping Information Secure: The CIA triad

Security's CIA triad:

- **Confidentiality**
- **Integrity**
- **Availability**



Security VS Safety

Security:

- Secure your computer just as you secure the doors to your home. Has mostly to do with the security measures and tools that you use.

Safety:

- Behave safely to protect against risks that come with technology. Has mostly to do with the way you behave when using computers or the Internet.

Topics to Cover

- **Security against:**
  - Viruses & Worms
  - Trojan Horses
  - Logic Bombs
  - Ransomware…

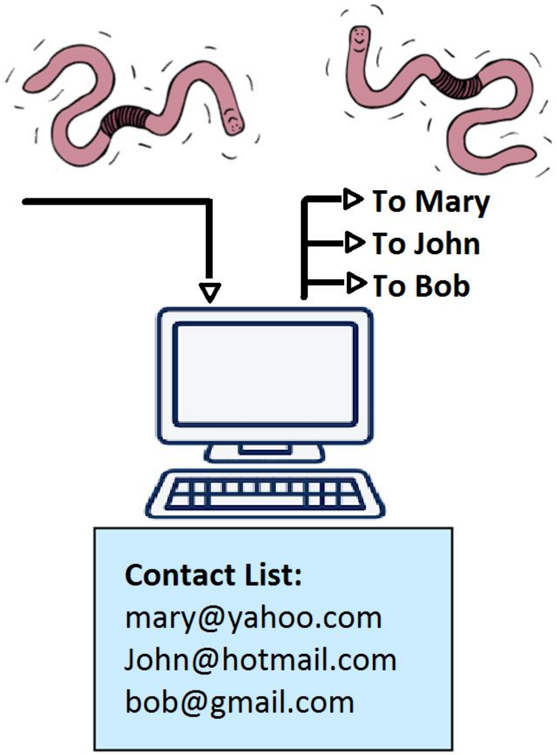
- **Safety against:**
  - Social Engineering
  - Phishing
  - Pharming
  - Malicious Websites…

Security threats

- **Virus**: Self-propagating malicious programs that attaches itself to other programs and the cycle goes on…

- **Worms**: Independent programs that can spread themselves without having to be attached to a host program

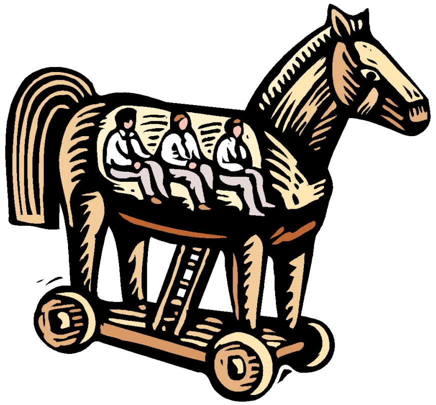
Transmitted mainly through download, e-mail attachments, flash drives.



Contact List:
mary@yahoo.com
John@hotmail.com
bob@gmail.com

Security threats

- **Trojan horses** breach your security while seemingly performing good functions.
  - Usually downloaded invisibly with a program requested by you.



- **Risks:**
  - Spies on your online behavior
  - Transmits your sensitive information

Security threats

- **Logic bomb**: a malicious software that is triggered at a certain time or by a specific event.

- **Backdoor**
  - Programming routine built into a system by its designer
  - Enables the designer to bypass security and sneak back into the system later to access info.

Security threats

- **Social engineering**: Using people skills to trick others into revealing private information.
- This type of attack is essentially non-technical but is one of the most dangerous.
  - Video to watch: watch an example of a phishing call.

This the System Admin. What is your password?

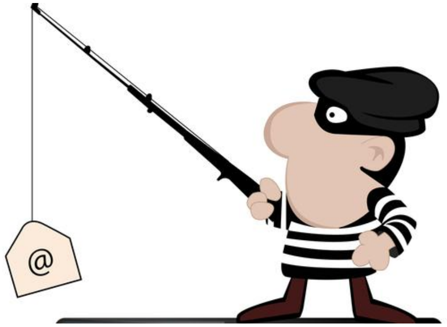
What elementary school did you attend? What is your pet’s name?

I am here to install an update on your computer

XYZ Bank has noticed a problem with your account…

Major types of social engineering

- **Phishing (fake email):** emails claiming to be from reputable companies to induce users to reveal sensitive information
  - usually putting time pressure



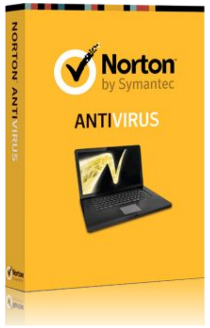
- **Pharming (Fake Website):** directing Internet users to a bogus website that mimics the appearance of a legitimate one.

The above are often used in conjunction: The link in the e-mail leads to a fake webpage which collects important information and submits it to the owner.

Safe & Secure User Practices

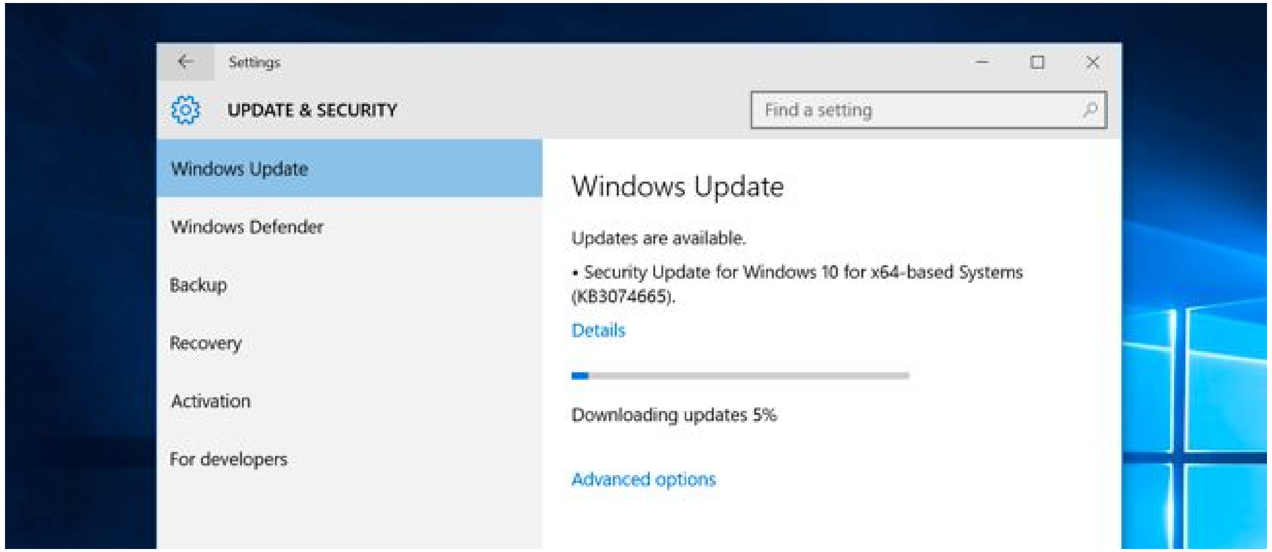
Anti-virus & anti-spyware

- Anti-virus software detects and destroys malware before any damage is done
- Install and keep antivirus updated
- Many free and paid options exist
  - Windows now includes one for free



Protect Your Operating System

- Install operating system patches or updates.
- Windows can be set up to automatically download and install updates.



Windows Update

Updates are available.

- Security Update for Windows 10 for x64-based Systems (KB3074665).

Details

Downloading updates 5%

Advanced options

Surfing the Web Safely

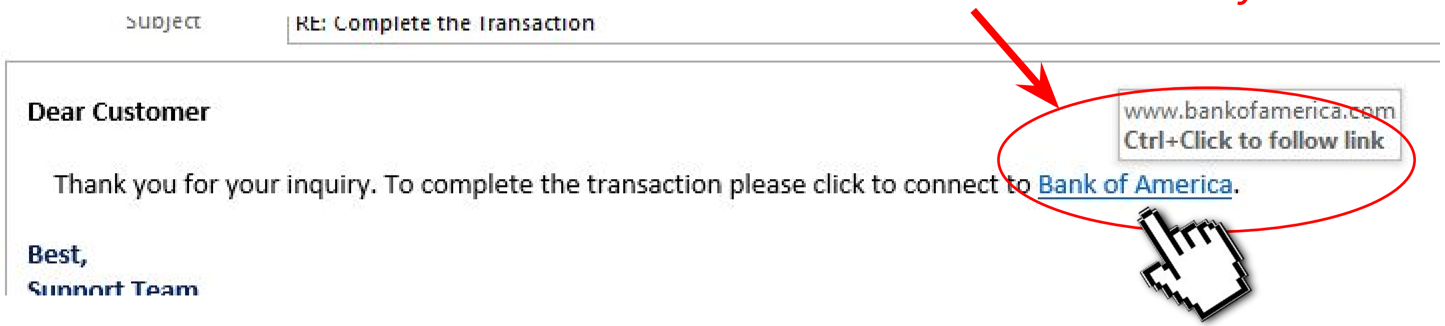
- Install program updates:
  - Application updates (Adobe…)
  - Browser updates (Chrome, Firefox…)
- Do not download programs from untrusted source
- Avoid suspicious websites
  - Do not assume certain types of websites are safe. Websites abut religion, for example, are among the more dangerous.
- Cover your webcam when not in use

Avoid social engineering & malicious software

- Do not open email attachments unless you are expecting them.
- Call the sender if in doubt.
- Do not click on links in emails unless you are absolutely sure of their validity.

BE SUSPICIOUS

Hover your mouse over links in emails to see the actual destination before you click.



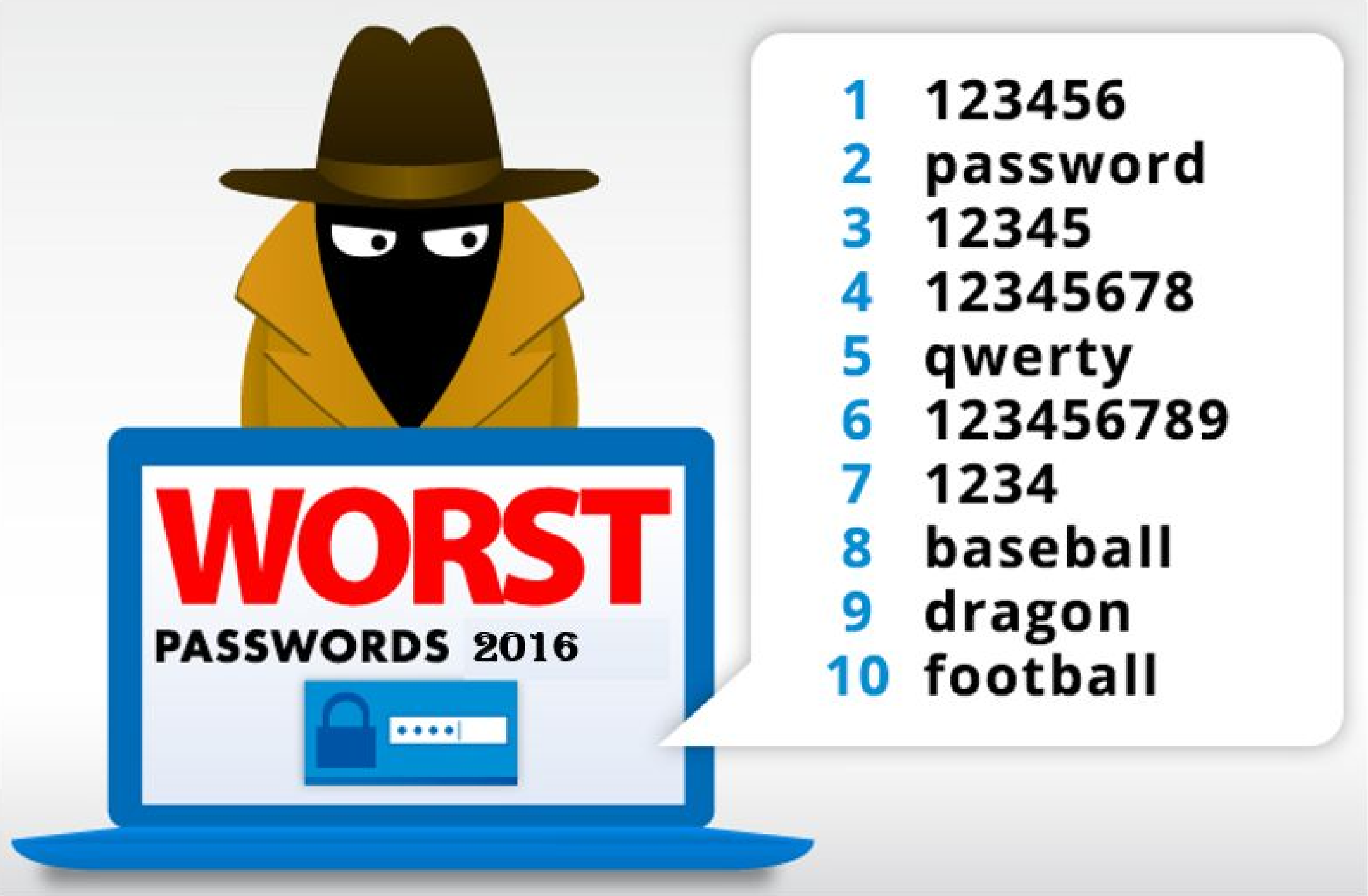
Subject RE: Complete the Transaction

Dear Customer

Thank you for your inquiry. To complete the transaction please click to connect to Bank of America.

Best,
Support Team

Use safe password



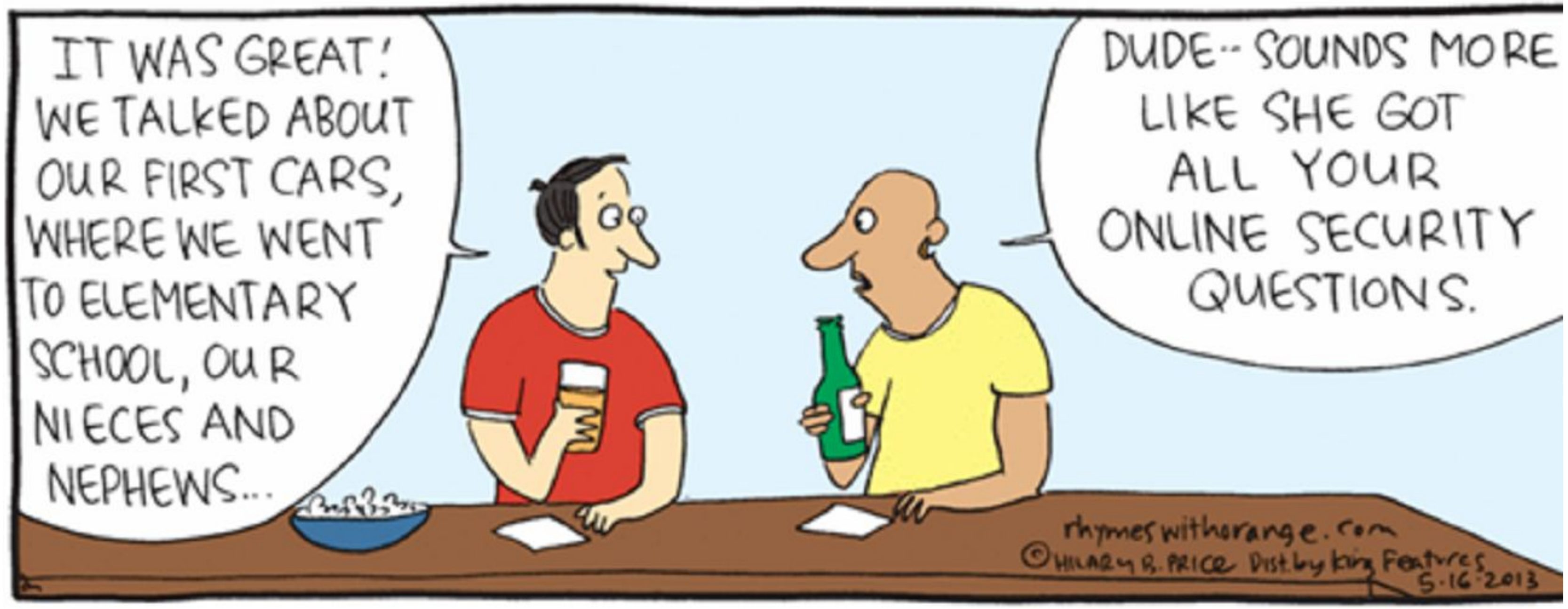
1	123456
2	password
3	12345
4	12345678
5	qwerty
6	123456789
7	1234
8	baseball
9	dragon
10	football

Passwords

- A good password is:
  - **Private**: it is used and known by you only
  - **Secret:** is not written on a piece of paper next to the computer
  - **Easily remembered:** so there is no need to write it down
  - **Is long and complex:** a mixture of upper/lowercase, digits…
  - **Not guessable** by anyone in a reasonable time
  - **Changed regularly:** preferably every 3 months
  - **Unique for every website:** so not all your accounts are compromised if one is.

****
*

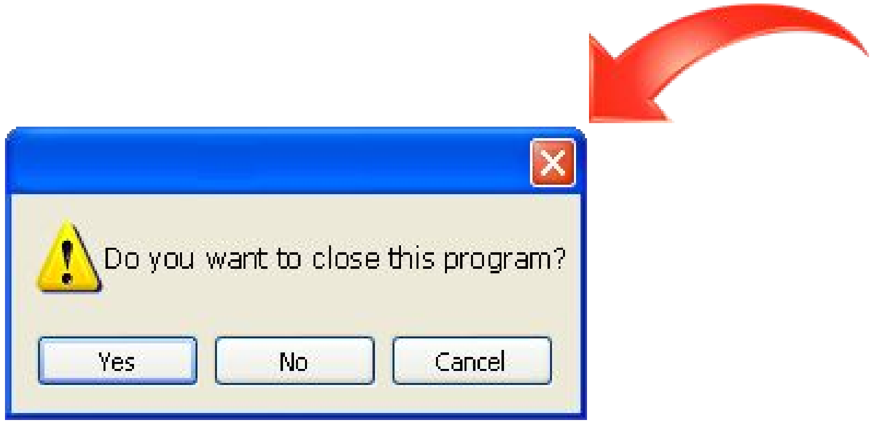
Use Safe Security Questions


IT WAS GREAT! WE TALKED ABOUT OUR FIRST CARS, WHERE WE WENT TO ELEMENTARY SCHOOL, OUR NIECES AND NEPHEWS...
DUDE-- SOUNDS MORE LIKE SHE GOT ALL YOUR ONLINE SECURITY QUESTIONS.
rhymeswithorange.com
©HILARY B. PRICE Dist. by King Features
5·16·2013

Apple: Don’t Blame iCloud for Celebrity Hacking

Other hacker tricks to avoid

- Never click “yes,” “accept” or even “cancel” on messages from websites/programs you do not trust
  - Use the X button to exit the message box
  - Or close the browser/program altogether.



Do you want to close this program?

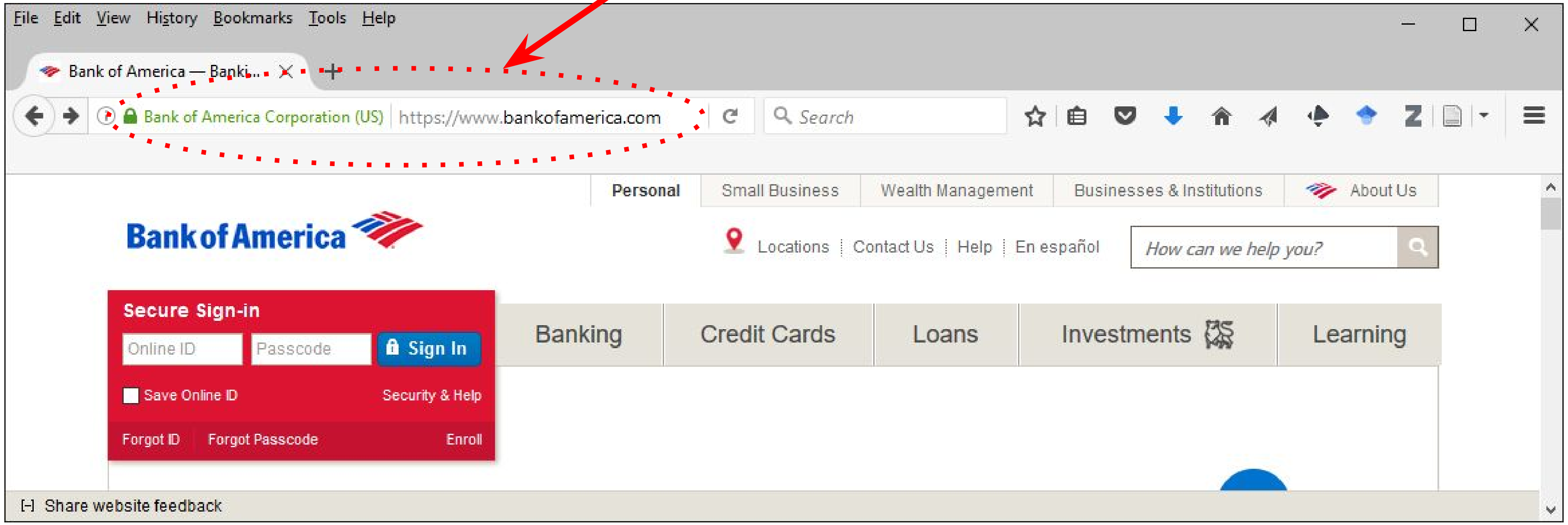
Secure online banking & business

- Avoid public computers to access sensitive websites/data
- Avoid public Wi-Fi as much as possible

✓ Check **Internet address** carefully

✓ Check for **https://**

✓ Check for the **lock symbol**



Backup

- No system can be 100% secured:
  - Hardware failure
  - Accidental deletion
  - Theft, fire, flood
  - Malware infections
- Identify important information and back them up.
- Always ask is your back-up:
  - Recent?
  - Off-site & Secure?
  - Process Documented?
  - Tested?

Thank you!