Malware Protection and Responsibility of user

Presented by:
Md. Abul Kalam Azad,CISSP,CISA,CISM,CRISC,CDPSE,CEH
Secretary, ISACA Dhaka Chapter
Email:kalam11@gmail.com

Importance of IT Security

- The internet allows an attacker to work from anywhere on the planet.

- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and your organization)
  - Sanctions or termination if policies are not followed

- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights

Implications for the Business

Immediate

- Loss of data
- Corruption or destruction of data
- Unauthorized access
- Account takeovers
- Compromised systems and applications
- Unavailability of services
- Reputation Loss
- Financial Loss
- Client Loss
- Regulatory Compliance & penalties.

Weakest Link?

- No matter how strong your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software

- **You** are the **weakest** link in computer security!
  - People are more vulnerable than computers

Why we are Vulnerable?

- Our desire to be helpful / Moral Duty
- Our tendency to trust people we don't know.
- Our fear of getting into trouble.
- Respect for Authority
- Chance of a Reward
- Cognitive biases: if someone seems kind and generous, perhaps one might believe that they are also intelligent and honest.

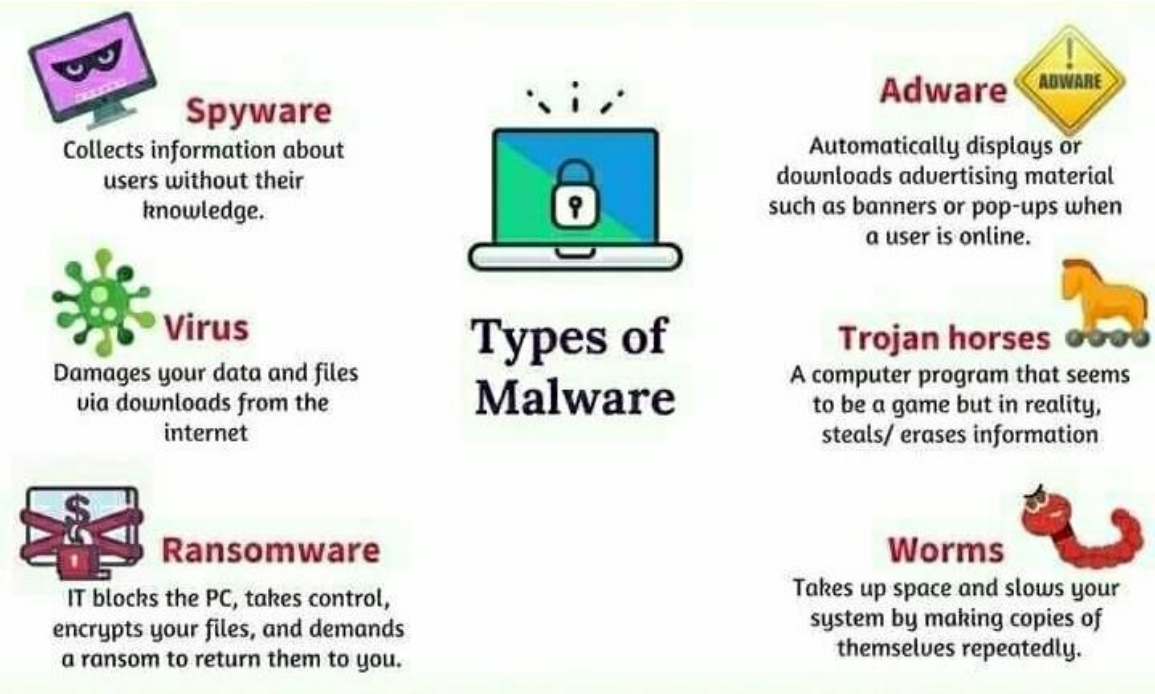
What is Malware?

- “Malware” is a malicious software that is designed to disrupt or damage your computer system.

- “Malware” is any kind of unwanted software that is installed without adequate consent.

- Hacker use malware for any number of reasons such as, extracting personal information or password, stealing money, or preventing owners from accessing their device.

Types of Malware



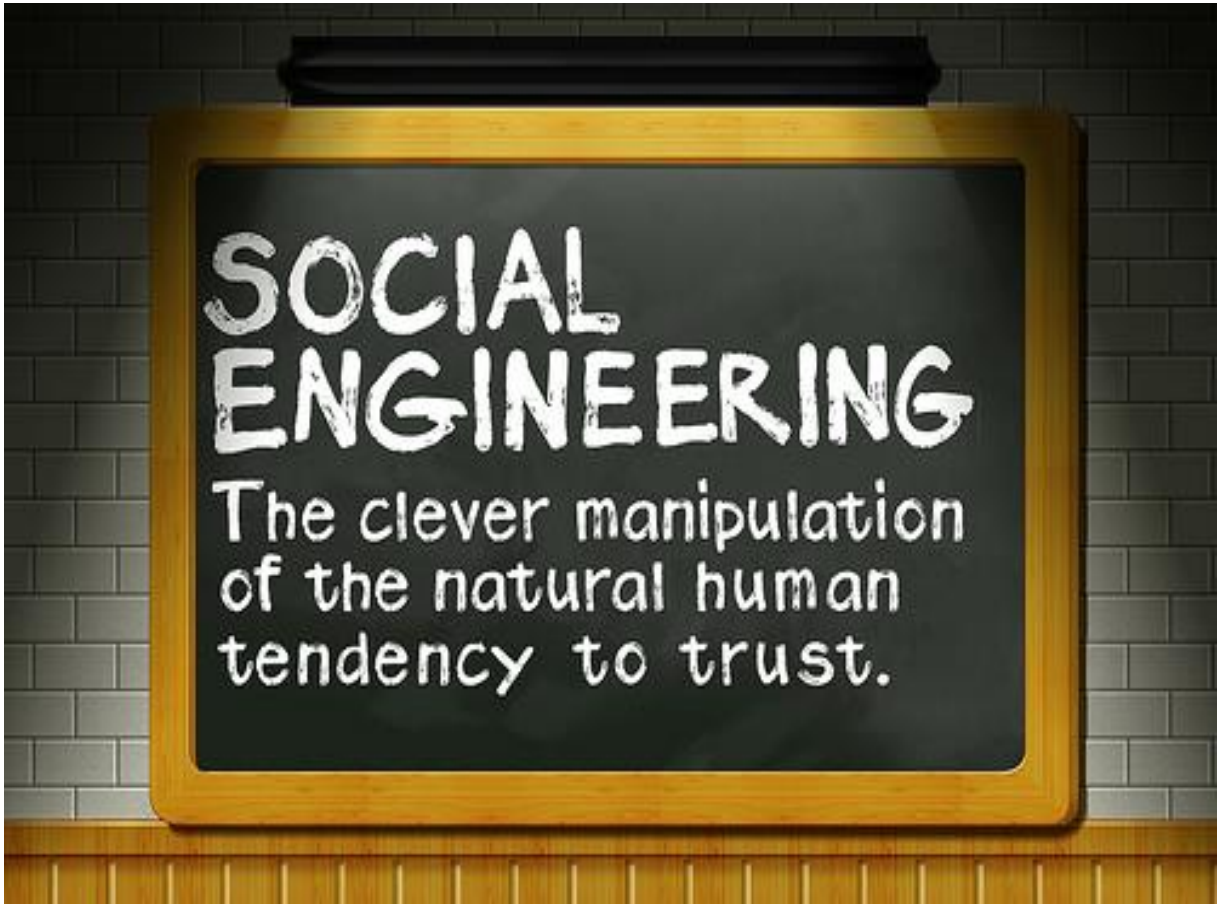
Ransomware screen

How malware get into your computer

- From contaminated media like USB drive, CD-ROM, DVD, etc.
- Through email and social networking sites
- Downloading a program from interr
- As part of another program.

Symptoms of malware infection

- Programs of your system start to load more **slowly**
- **Unseal files appears** on your hard drive or **files disappear** from your system
- Browser, word processing applications, or other software exhibit **unseal operating characteristics**
- **Pop-ups** suddenly appear, sometimes selling security software
- The **mouse pointer** moves by itself.
- **Changes** to your browser **homepage/start page**.
- The computer spontaneously **shuts down or reboots**.
- System suddenly doesn't reboot or gives **unexpected error messages** during startup


SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.

Social Engineering

Manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Why Talk about Social Engineering?

Social engineering is a component of the attack in nearly 1 of 3 successful data breaches, and it's on the rise.


Personal
Data

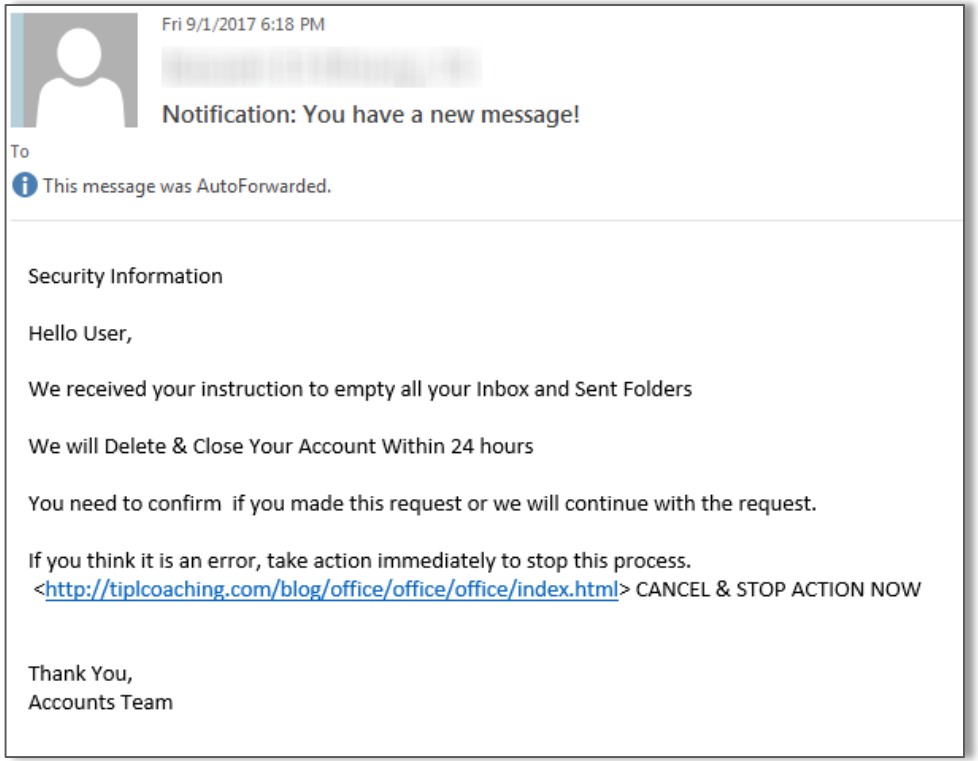
Phishing

Attempts to get users to provide information or perform an action

Tips For Identifying Phishing Attempts

- Asks to update account information via email
- No verification image or varying layout designs
- Provides unfamiliar hyperlinks

Phishing: Counterfeit Email



Fri 9/1/2017 6:18 PM

[redacted]

Notification: You have a new message!

To

This message was AutoForwarded.

Security Information

Hello User,

We received your instruction to empty all your Inbox and Sent Folders

We will Delete & Close Your Account Within 24 hours

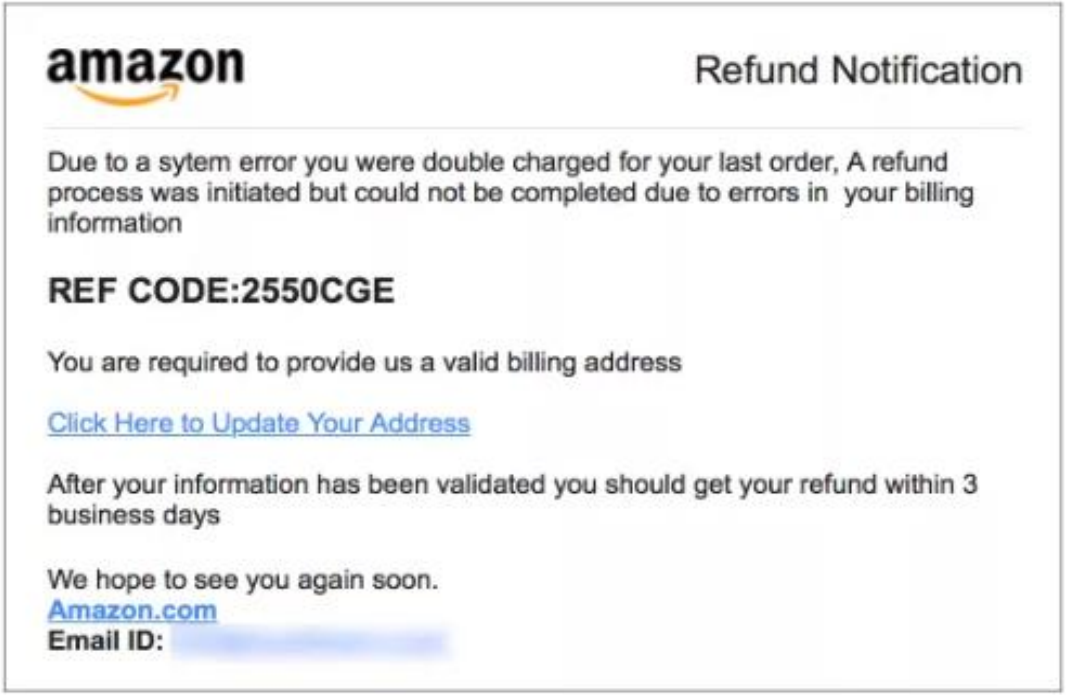
You need to confirm if you made this request or we will continue with the request.

If you think it is an error, take action immediately to stop this process.
<http://tiplcoaching.com/blog/office/office/office/index.html> CANCEL & STOP ACTION NOW

Thank You,
Accounts Team

Phishing: Counterfeit Email

Phishing: Counterfeit Email



amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

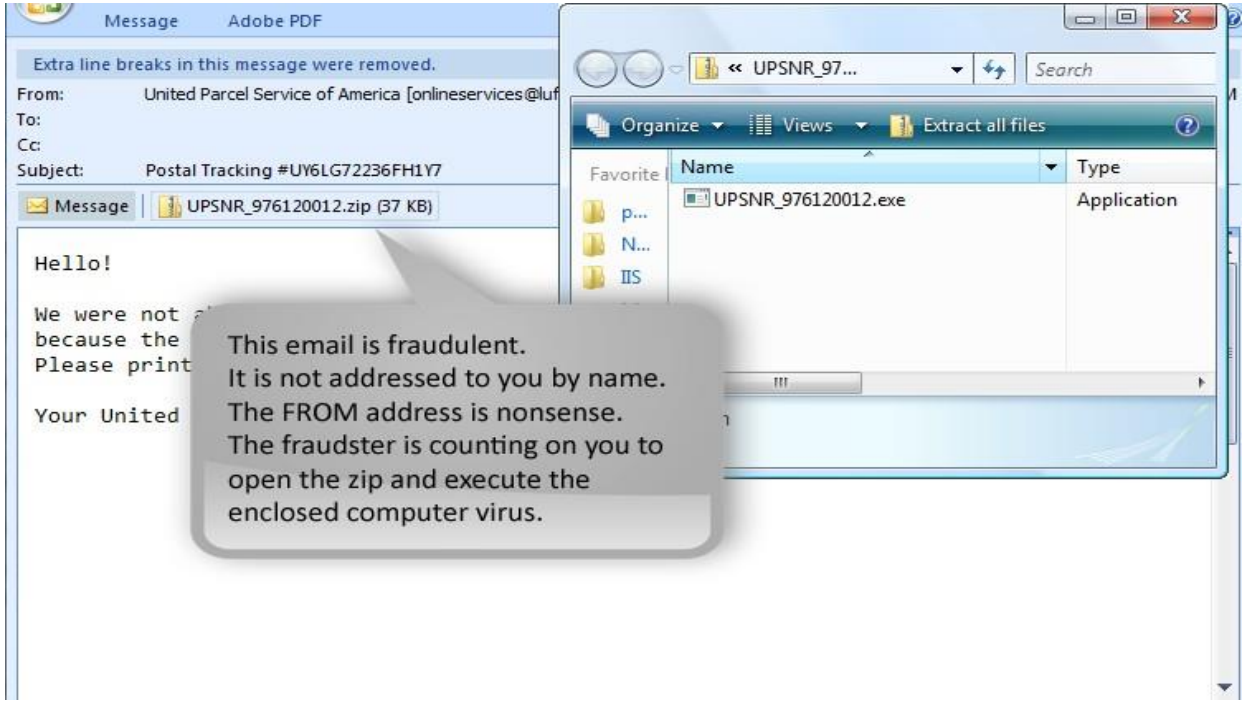
You are required to provide us a valid billing address

Click Here to Update Your Address

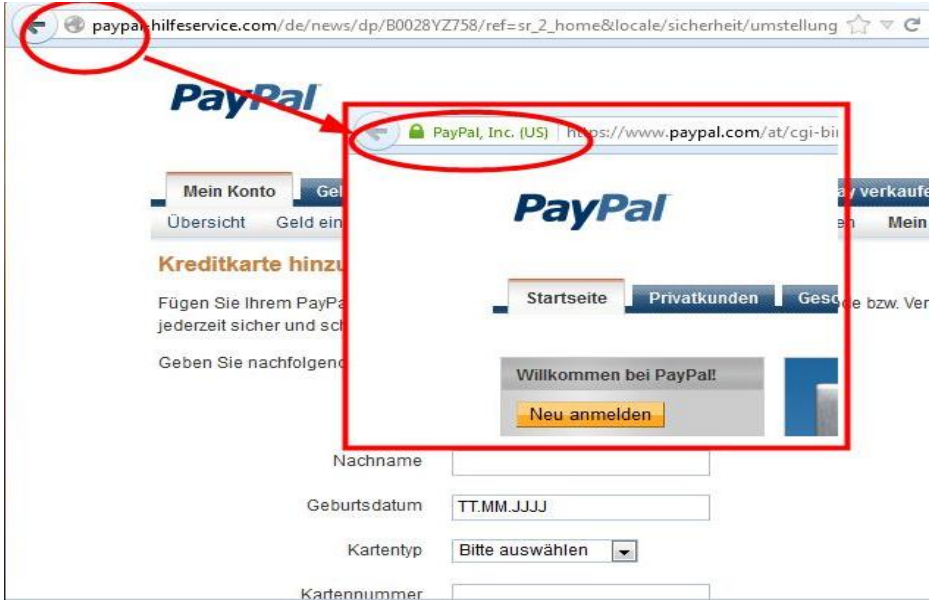
After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID:

Phishing: Counterfeit Email



Pharming: Counterfeit Web Pages



- The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.
- The counterfeit web page looks like the real thing
  - Extracts account information

Check it – Don't Click IT

- **Don't click links within emails** unless sent from a reliable source, and only after verifying the URL
- **Don't open attachments** unless you are sure of the sender and expecting something from them
- **Assess the content/context** Does it make sense, coming from the sender?

People love USB Stick!

I found it in the car park …

… just wanted to see what was on it …

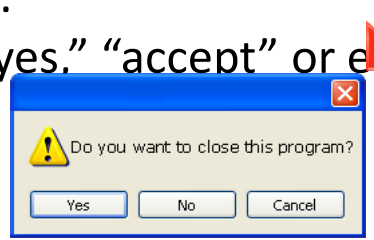
Enticement Examples

A folder with enticing title/label left on ground outside an employee entrance with a USB thumb drive taped inside.

- USB, CD or DVDs left in conspicuous spaces.
- May be accompanied by fake paper files
- Curiosity beats caution

Avoid Stupid Hacker Tricks

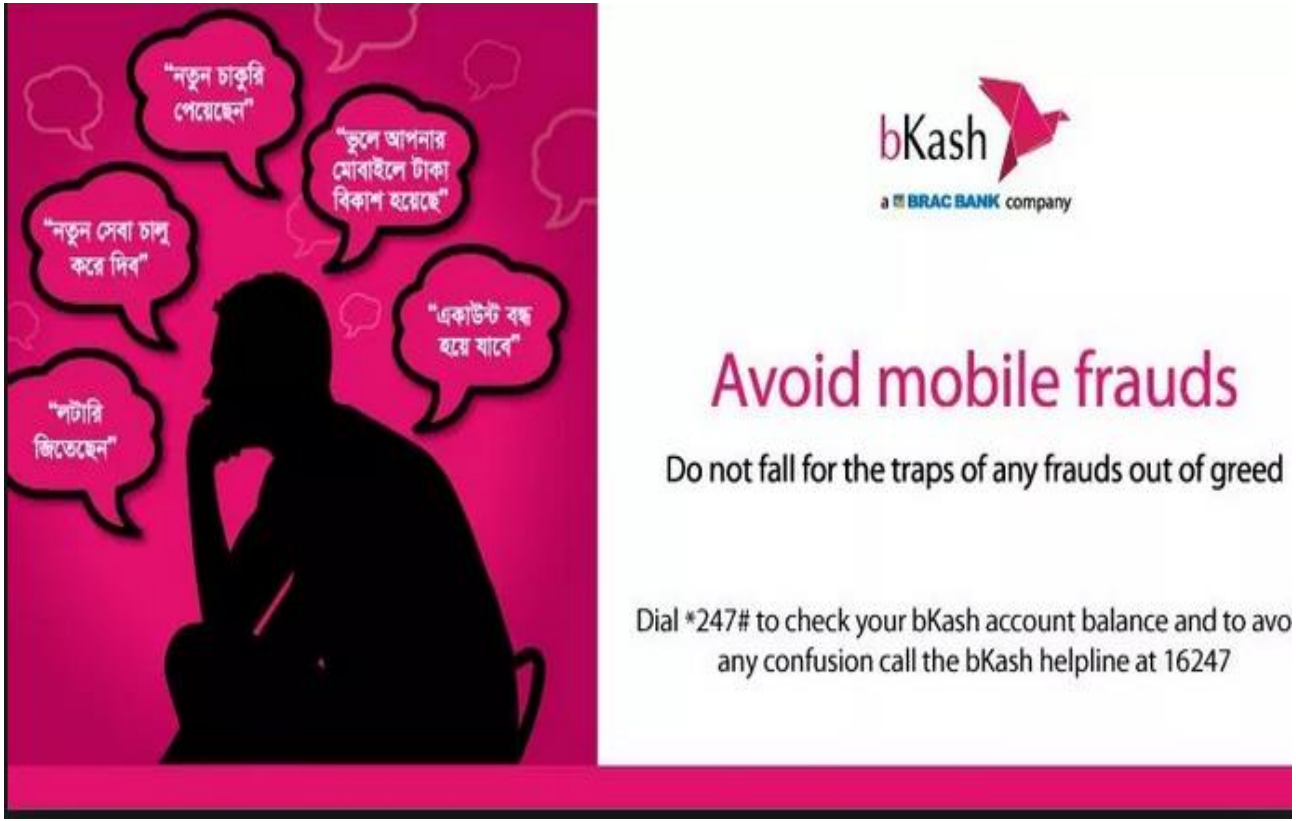
- Be sure to have a good firewall or pop-up blocker installed.
- Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the 'X' in the upper corner.
- Never click "yes," "accept" or even "cancel."

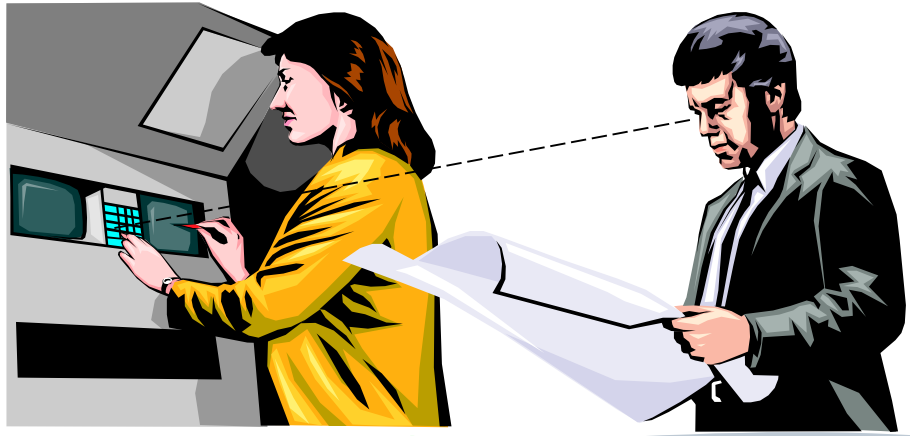


- Infected USB drives are often left unattended by hackers in public places.

Dumpster Diving

- Scouring through discarded items
  - Calendars & Day planners
  - Handwritten notes
  - Phone & Email Lists
  - Operation manuals or procedures
  - System diagrams & IP addresses
  - Source code


"নতুন চাকুরি পেয়েছেন"
"ভুলে আপনার মোবাইলে টাকা বিকাশ হয়েছে"
"নতুন সেবা চালু করে দিব"
"একাউন্ট বন্ধ হয়ে যাবে"
"লটারি জিতেছেন"
bKash
a BRAC BANK company
Avoid mobile frauds
Do not fall for the traps of any frauds out of greed
Dial *247# to check your bKash account balance and to avo
any confusion call the bKash helpline at 16247



Shoulder surfing takes many forms. Some may not be obvious.


Time for a
new password
Social
Security #


My password is so strong nobody can guess it!
No, we just read it off the sticky note you have on your monitor.

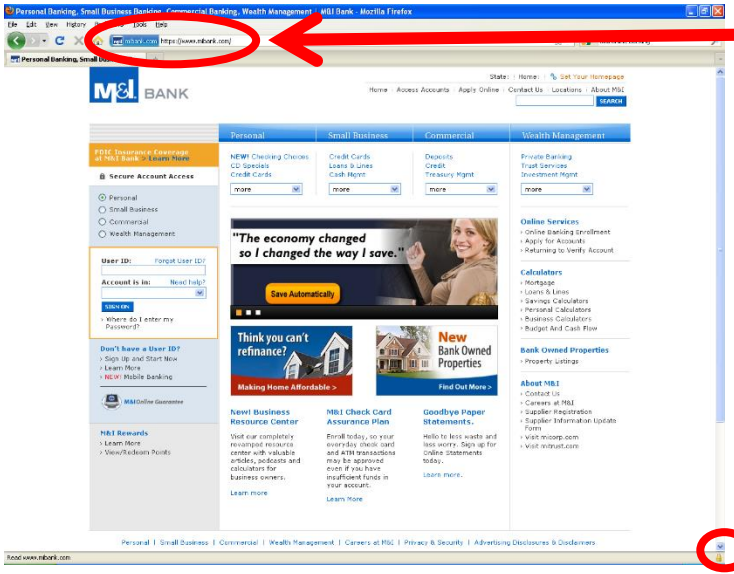
Use Strong Passwords

Make passwords easy to remember but hard to guess

- Best Practice:
- Be at least ten characters in length
- Must contain characters from at least two of the following four types of characters:
  - **English upper case (A-Z)**
  - **English lower case (a-z)**
  - **Numbers (0-9)**
  - **Non-alphanumeric special characters ($, !, %, ^, …)**
- Must not contain the user's name or part of the user's name
- Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.

Secure Business Transactions

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.



Backup Important Information

- No security measure is 100% reliable.
- Even the best hardware fails.
- What information is important to you?
- Is your backup:

Recent?
Off-site & Secure?
Process Documented?
Encrypted?
Tested?

Physical Security Awareness

Physical Security

- **Wearing Badges**
- **Never** share your **Access card**, code or key.
- **Tailgating**.
- Signing in and **escorting** visitors.
- **Challenging strangers**.
- **Don’t** hold secure **doors** open for strangers.
- **Lock up** any sensitive **material** you operate with.
- **Don’t** leave any devices **unattended**.
- **Lock** your **Devices** when unattended.
- Follow the **clean desk policy**.
- **Report** your IT department about the **loss of dev**ices**.**


Thank You!