Why Information Security

Information security (IS) is the practice of protecting information from being leaked, changed, and accessed without approval.

MCB Bank is committed to ensure security of internet banking systems for its customers through;

• State of the art network and application layer firewalls;

• Secure communication on all internet banking channels;

• Development and maintenance of secure internet banking applications;

• User lock-out after 05 invalid password attempts;

• Automatic log-out after 15 minutes of inactivity;

• SMS alerts

Protect your password: it is your identity in digital world

YOUR PASSWORDS SHOULD:

• not be based on guessable information such as your name, personal telephone number, birthday or other personal information;

• not be a dictionary word;

• be kept confidential and not be divulged to anyone;

• be memorized and not recorded anywhere e.g. sticky notes;

• be changed regularly, or when there is any suspicion that it has been compromised or impaired;

• not be same for different websites, applications or services, particularly when they relate to different entities;

• avoid using the same details that you use to access other services such as email, other Internet sites/ISPs, ATM PIN, or Phone Banking TPIN;

• for better security, it is highly recommended to adopt 8-16 alpha-numeric character set consisting of both letters and numbers, lowercase and uppercase, e.g. IcneL9305.;

• must not contain 3 or more consecutive identical characters, e.g. "aaa" or "111", etc.;

• must not contain 4 or more consecutive identical characters as part of your Password, e.g. "1234" or "abcd", etc.

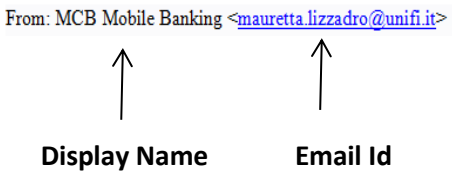
Basic DOs and Don'ts	
DOs:	DON'Ts:
✓ always use licensed software and tools; ✓ install anti-virus and keep it updated; ✓ keep your operating system, and applications up-to-date; ✓ enable personal firewalls; ✓ enable password protected screen saver to start after 15 minutes of inactivity; ✓ lock your computer when you are away from it; use Windows logo key + L or Ctrl+ Alt + Del key; ✓ use secure WIFI connections by password protecting it; ✓ change WIFI key regularly ✓ disable file and printer sharing on your operating system; ✓ only give your email address to the people you know; ✓ log-off internet banking applications / system when not in use; ✓ regularly check your last internet banking login date & time, balance and transactions;	✘ access any other website within the same internet browser session when using MCB bank's Online Banking; ✘ save your username & passwords in your browsers; ✘ reveal the OTP or OTP SMS received from the bank; ✘ open suspicious e-mail attachments sent by strangers; ✘ use freeware, shareware software, unlicensed copies of proprietary software and chat software (such as Skype, Google Talk, Yahoo Messenger, etc.) as harmful viruses are spread through these programs; ✘ leave your wireless & Bluetooth turned on when not in use; ✘ use public systems for financial transactions, unless unavoidable.

E-mail Safety Tips

- Discard and report at help desk regarding any email that asks for your personal information such as Full Name, DOB, Bank Account Number, CNIC, Card number, and CVV code. This seemingly benign information can be misused for un-authorized access to your accounts;

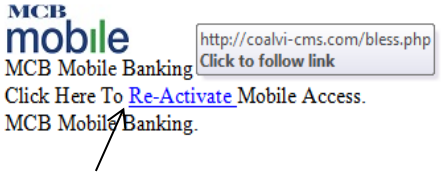
- Fake e-mails entice you to respond quickly; don't become preys to them;

- Always check for the email address despite of display name, display name can be easily changed, email address can't be!



Display Name **Email Id**

- Don't open link in the email, if essentially required, browse google and get the actual link



fake link behind text will be shown when hovering your mouse over it

- Verify attachments (scan with an antivirus) before opening because attachments may carry viruses

- Be aware of "Bcc:"

What is Social Engineering?

Gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with company employees and insiders.

Criminals know that today it is much harder to break into networks, applications, and physical facilities. So by default, the human being has now become the "weakest link" in security.

How does Social Engineering work?

Social engineers (attackers) leverage trust, impersonate (pretend to be someone else), get knowledge of internal processes, and sometimes threats, to capture unauthorized information or access. It is all about taking advantage of others to gather information and infiltrate an organization.

Examples of Social Engineering:

- The attacker poses to be a legitimate user or superior manager: "This is the ROM/Vice President and I need…" In this case, the administrator or an end user may feel threatened by the caller's authority and may provide the information out of fear;
- The attacker may gain the user's trust by posing as a technical staff member offering help to fix a computer problem;
    - "Hi, I'm Farrukh, from the service desk; please confirm your user name & password" "Hi, I received your request to change your password, please tell me your previous password so do I help you."

Social Engineering Techniques

Pretexting is the act of creating and using an invented scenario (the pretext) to persuade someone to release information or perform an action and is typically done over the telephone.

Phishing is a technique of fraudulently obtaining private or sensitive information. The phisher sends an email that appears to come from a legal business address requesting "verification" of information. The user may be asked to change the password of a specific email address or an ATM card PIN code of an ATM account.

Spear phishing targets specific groups of people or specific titles and designations such as CEOs. One major spear phishing attack offered company CEOs useful legal information and actually installed a virus on the user's machine!

Vishing scams use phone calls instead of email - and VOIP phones are favored because they are hard to trace and track.

SMSishing scams use SMS text messages instead of phone calls or email messages.

Shoulder surfing refers to using direct observation techniques such as looking over someone's shoulder to get information. Shoulder surfing is particularly effective in crowded places.

Dumpster diving is the practice of searching through commercial or residential trash to find useful items that have been discarded by their owners.

Spoofing attack is a situation in which a person or program illegally modifies the source address or other information to avoid being traced. For example, Facebook is one of the most spoofed websites in the world which has several security loopholes.

Spam refers to any unwanted email or SMS message you receive. Most spam is simply correspondence which you didn't request for, mostly advertising and marketing materials. It is annoying, but they are no real security threats as long as you do not respond or click on any links provided in unsolicited emails.

ATM Scams are a common social engineering technique. One simple trick is to manipulate the ATM machine to malfunction and capture your card. A nearby stranger says to you, "the same thing just happened to me. Here, let me help." In the process, the stranger tricks you into sharing your ATM PIN. After you leave, he will retrieve your "stuck" card and empty your account.

How to protect against social engineering attacks

• Know how to detect phishing attempts and beware of suspicious email attachments;

• Ask questions and do not trust strangers;

• Criminals are targeting social networking sites such as Facebook™, Twitter, MySpace and Bebo to steal personal information - so be careful with what you share online;

• Don't publish details that can identify you. They include birthdates, phone numbers, addresses and full names;

• Limit your profile. Consider restricting your profile to friends and family only;

• Make sure you know & trust the person before accepting friend request on social networking sites;

• Shred personal information and do not leave it easily accessible on your desk / printer, this may be used to steal your account information;

• Make sure you understand the privacy policy of each site as some may sell users' email addresses, leaving you susceptible to phishing and spam;

• Do not let strangers come near you while at the ATM keypad while entering your ATM PIN;

• Don't be caught by the spammers' favorite tricks, such as the use of subject headings like "Remember me?" that try to trick you into thinking you should know the sender;

• Be cautious when opening emails and email attachments, especially when receiving emails from strangers;

• Simply delete emails from unknown senders or dubious sources because your reply or click on any link in the email message from an unknown source, you are confirming to the unknown sender that your email address is a valid one;

Know your threats

What is a malware, spyware, adware or Trojan?

- The terms malware and spyware refer to any piece of software installed on your computer without your permission. Malware refers to software that causes damage to your computer;
- Spyware gathers information from your computer without your knowledge;
- Adware installs software that displays advertisements on your computer;
- Trojans specifically refer to software that, once installed, secretly installs another piece of software;
- Once installed, the software collects information or interrupts traffic to web sites and other critical services.

What do they do?

Once installed, a piece of software may activate viruses that:

- Interrupt and disable basic system operations;
- Capture and transmit keystrokes that may reveal passwords and other information;
- Capture and send emails and other personal information;
- Hijack your network connection, and then use it to send more malware.

How does it work?

Most of the time, customers install malware or adware by accident when they click on a link they find in an email message or web page. Malware or spyware may also be unknowingly installed with software from an unreliable source. Such malware or spyware may even be installed together with dubious anti-virus software.

What can you do to protect yourself from malware/spyware?

Real protection from malware and spyware require both technology and knowledge on what to look out for when you use the Internet.

- Install and run reliable anti-spyware/anti-virus software. Be aware of the installation process and do not click on links that direct you to download other software;
- Make sure you are accessing links only from trusted sources;
- Monitor the performance of your machine carefully. If it starts to run slowly, or web traffic begins to behave erratically, run a scan immediately;
- Malware is designed to steal user information by altering the look and feel of the website. E.g. If your computer has been infected with malware, you may be prompted to enter your online banking username, password and One-Time Password (OTP) ALL in one screen. The correct login method requires you to enter your username and password only.

Man-In-The-Browser Attack

- Please be highly aware of a recent online threat known as a Man-In-The-Browser (MITB) attack, where an attacker takes control over a customer's connection and transmits counterfeit screens to the customer in attempt to capture and manipulate customer data;
- A frequent MITB attack scenario involves the attacker taking control over a customer's login session. The attacker transmits screens similar to the online banking screens requesting the customer to wait while their details are being verified. During this, the attacker would initiate a request for adding payee or updating personal information while the customer's account is being compromised. An SMS containing a One-Time Password (OTP) is sent to the customer's mobile phone as part of the process. More counterfeit screens are transmitted to the customer to prompt the customer to key in the OTP in order for the attacker to proceed with payee addition and/or personal information update;
- Stay vigilant, and do not proceed if you notice an unusual screen or message during your online banking login session.
- Do not act on an SMS containing an OTP that you have not requested for, review your existing payee list for any unauthorized additions.

What are viruses?

Viruses are small software applications designed to cause damage to the information on your computer. They may also try to gather sensitive information which can allow others to gain access to your accounts. Like viruses passed between humans, computer viruses usually spread from customer to customer.

What do they do?

Some viruses are malicious, designed to corrupt files and cause problems. Some may attempt to access your email or contacts and try to replicate your email identity, while others may look for sensitive information stored on your computer.

How does it work?

Most viruses are spread through emails or shared files. When a customer clicks on a link, thinking that they're opening a photograph or website, the virus gets activated and goes to work right away, causing trouble.

How can I protect myself from viruses?

Your best defense against computer viruses is to keep your anti-virus software updated regularly.

- New viruses are constantly being created;
- Developers of anti-virus software are constantly updating their virus definitions to tackle new threats;
- Your anti-virus software needs to be updated with these new definitions to protect your computer against the latest threats;
- Be careful about opening links and files that show up in your inbox. People can send viruses without knowing that they've been infected, so even emails from family and friends should be handled carefully;
- Use an email program that scans email attachments for viruses;
- Never open email attachments or links from unknown senders;
- Be careful of emails that contain links to external content or downloads, and never click on links that end with ".php" or ".exe" unless they're from a trusted source.

Protect Your Phone

Smartphones make up an integral part of our lives these days. With mobile payments and banking becoming increasingly popular, it's important to apply the same security measures to your mobile phone as you would to your computer. In the wrong hands, your mobile phone could give the wrong person access to your accounts and ultimately your money. Keeping your phone updated and secure is the first step towards real mobile security.

- Always download apps from trusted sources;
- Keep your phone's Operating System (OS) and apps updated;
- Restrict access to your phone with a password or PIN
- Set your phone to lock after a short period of inactivity
- Do not store passwords or accounts numbers on your mobile phone
- Limit the amount of personal details or contact information that you store in your phone, as criminals may be able to retrieve them if you happen to lose your phone
- If you lose your phone, report it to CPLC, Police and PTA, they will get some basic info along with the IMEI number of your lost mobile set, and will request all the mobile operators to block this IMEI on their networks;
- Make a note of your phone's IMEI number (dial *#06# to get it). This makes it easier to disable a stolen phone
- For iPhone users, never jail-break or crack the device. Activate encrypted backup in iTunes, and turn on the passcode lock for the phone
- For Android users, never root or crack the device
- Never leave the MCB mobile banking app running in the background. Smart phone users should always log out after using the app

Reporting an Information Security Incident

In case of any personal fraud related issues like user-id locked, loss of security credentials, fraud or identity theft, please contact by emailing us at info@mcb.com.pk or calling us at +92-21-111-000-622 or +92 0800 62272.

Call center standard verification process is followed for re-authentication of internet banking users.

For any complaints, please contact MCB Bank helpline or your branch.