

SECURITY TIPS

Overview:

While we have taken all possible measures to ensure security and confidentiality of our online trading system, you play an important role in protecting your personal information and Passwords. You may have to protect your information at all times while performing trading over the internet or during your normal trading activities by simply following these tips:

Protect your Password and Personal Information:

1. Do not use passwords that are easy to guess, e.g. your name, your date of birth, your telephone number(s), etc
2. Use a combination of upper and lower case letters as well as numbers
3. Do not share your password with anyone and do not use the same password for other websites
4. Change your password frequently and never write it down in any where
5. Always log into Internet trading via our sites at the following addresses: <https://ebroker.emiratesbank.com> and not through other links
6. Avoid logging into Internet for trading from Internet Cafés, Libraries or public sites
7. Always close the window once you have logged out of your Internet trading session

Important: No one at Emirates International Securities (ENBDS) will ever ask you for your internet-trading password. If someone does ask you for it, they do not represent ENBDS and under any circumstances, you should not provide this information.

Protect your Computer and Internet session:

1. Never share your computer
2. Use a password on your PC to prevent unauthorized access to your information
3. Be wary of opening email messages from untrustworthy sources, especially if they contain attachments
4. Do not reply to emails that request your personal information. They may appear to come from a trusted friend or business, but they are designed to trick you in disclosing sensitive personal information
5. Use personal firewalls and anti-virus software
6. Avoid downloading software such as screen savers, desktop themes, games, and other executable type programs from websites that are obscure or unidentifiable. These programs may contain Trojan viruses that would enable hackers to monitor or take over your PC
7. Disable all unnecessary services running on your computer
8. Always verify that the site is the genuine Emirates NBD/ENBDS site
9. Do not leave your internet trading session unattended at any time
10. Before you start your internet trading session, ensure that all other internet sessions are closed. If your internet trading session is open, we recommend that you do not open other internet browsers at the same time

Please contact our Customer Service Helpdesk on 043160100 or ENBDS Head office on 043119111 in case you receive fraudulent emails or require any assistance in using our Internet trading service.

More on Security

Protecting your information properly is a shared responsibility of both you and ENBDS and ENBDS is bound to maintain confidentiality according to our security procedures and code of ethics. You also play an important role in keeping this information secure too.

Recommendations for Password Security

Pass phrases and Passwords

"If you've ever lost your wallet, you know the sense of vulnerability that comes with it. Someone might be walking around with your identification, pretending to be you. If someone steals your passwords, they could do the same thing online. "

Weak passwords

You probably already aware of not creating passwords using any combination of consecutive numbers or letters such as "12345678", "lmnopqrs", or adjacent letters on your keyboard such as "qwerty." And you've probably heard that using your login name, your spouse's name, or your birthday as your password are also big no-nos, or that you should never use a word that can be found in the dictionary, in any language? & even common words spelled backwards (Although at times becomes hard to remember)

Step 1: Create strong passwords that you can remember

The advice that we should follow is to come up with a completely random combination of numbers and symbols. We all know that a strong password is the one that, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess. This is the right approach but at times we tend to make the password complex for us to remember and resultant, we take a note of it on paper. Doing so we defeat the purpose of Strong Passwords, why? Chances are you would write it down and keep it in the top drawer of your desk and then it's No longer such a Great Password after all.

The easiest way to create a strong password is to come up with a pass phrase. A pass phrase is a sentence that you can remember, like "My son Aiden is three years older than my daughter Anna." You can make a pretty strong password by using the first letter of each word of the sentence. For example, msaityotmda, well we all know that we have to include numbers special characters for it to be valid.

You can make this password valid & stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. Substitute a @-sign instead of a, \$-sign instead of an s,! Instead of an l or 1, (for c, 0 for o and so on. Well, you were not the first person to do that.)

For example, using the same memorable sentence and a few tricks, your password is now M\$@!3y0tmd@ If you still think that is too hard to remember, you could try a more common phrase, such as "You can't teach an old dog new tricks." If you are using a common phrase, make sure to inject at least one number or symbol into the password. Such as U (t@0DnT.

Step 2: Keep your passwords a secret

Keeping your passwords safe means you have to keep them secret. Do not give them to friends and do not write them down and keep them at your desk or in an unprotected file on your computer. Your desk and that friend may not have the best motives when it comes to your privacy.

You should also be wary when giving them to the Web Site where you created the password in the first place. A new way in which hackers trick people into giving away their passwords and other personal information is through a scam called "phishing." Phishing is the practice of sending millions of bogus e-mails that appear to come from popular Web sites. The e-mails look so official that many people will respond to requests for their login name and password

Recommendations for Home Computer Security

Task 1 – Install and use an Anti-Virus Program

A virus is a program that runs on your computer system without your permission. This means that when the virus runs, somebody else is using your computer possessions. A virus may also be destroying your files or disclosing them to others who aren't otherwise allowed to see them. An anti-virus program attempts to stop this from happening.

Task 2 – Keep your system Patched

Programs that need to be patched are weak spots through which intruders can more easily gain access to your computer possessions. Patching attempts to eliminate this kind of access. To protect your possessions, you need to keep all of the software you've purchased patched with all of the patches provided by the vendors who write that software. Vendors will tell you where to find and how to patch the software you have purchased from them.

Task 3 - Use Care When Reading Email with Attachments

Email attachments that you were not expecting are usually viruses, so the comments from Task 1 also apply here. Whether they are viruses or not, they are most often programs that run on your computer system without your permission. By using care, you are attempting to stop running unwanted programs on your computer system.

Task 4 – Install and Use a Firewall Program

A firewall program attempts to keep outside access out and limits inside access to outside resources. That is, it works like your locked front door that keeps unwanted people out and your toddler in. If intruders can't get to your computer resources, they can't use them for their purposes.

Task 5- Make Backups of Important Files and Folders

If a file or folder is destroyed accidentally, by an intruder, or in some other way, then a backup provides another copy. You are keeping what is yours by having more than one copy.

Task 6- Use Strong Passwords

These days, most of computer access users' login selecting a strong password makes it harder for intruders to access your computer resources, because those passwords are harder to guess.

Task 7 - Use Care When Downloading and Installing Programs

The Internet is a powerful resource for finding and using the work of others to enhance your computing resources. Programs are one example. However, not all programs on the Internet are what they say they are. Some programs are viruses like those described in Task 1, while others are like the email attachments described in Task 3. By taking care before downloading and installing these programs, you are trying to improve the chances that these programs are what they say they are, will do to your computer resources what you want them to do, and will do nothing more.

Recommendations for Email Security

Below are tips for using your email more safely.

1. **Minimize the use of attachments**

Copy and paste text as often as possible.

2. **Question unsolicited document**

Unsolicited bulk mail and commercial email can put you and your organization at risk. Questioning it means not opening it, not passing it on, but make sure to notify your system administrator immediately.

3. **Never respond to spam email**

For a spammer, one "hit" among thousands of mailings is enough to justify the practice. Instead, if you want a product that is advertised in a spam email, go to a Web site that also carries the product, inquire there, and tell them you do not approve of spam methods and will not patronize a company that uses spammers.

4. **Never respond to the spam email's instructions to reply with the word "remove"**

This is just a trick to get you to react to the email. It alerts the sender that a

human is at your address, which greatly increases its value. If you reply, your address is placed on more lists and you receive more spam.

5. **Never sign up with sites that promise to remove your name from spam lists**

These sites are of two kinds: (1) sincere, and (2) spam address collectors. The first kind of site is ignored (or exploited) by the spammers, and the second is owned by them. In both cases, your address is recorded and valued more highly because you have just identified it as read by a human.

6. **Keep your virus protection up-to-date**

Always make sure that the virus protection in your computer is in use and up to date.

7. **Question executable programs received via email**

This is the common way of passing viruses. Do not open them, do not pass them on, and notify your system administrator if you receive them.

8. **Disable macros on your machine**

To do this, you will need to open the application on Word 2000, select Tools, then select Macros, then select Security, and then checked High: Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.

9. Make sure that file extensions are viewable

This will alert you to files of the following types: .exe, .vbs, and .shs. To view file extensions in Windows select the Start menu, then select Settings, then select Control Panel, then select Folder Options, then select View, then UNCHECK the command that reads Hide File Extensions for Known file Types.

10. Notify the person you received an infected file from

This helps them to correct the problem within their system before passing the virus on to other users.

11. Monitor your transactions.

Review your order confirmations, account operations and trading statements as soon as you receive them to make sure that you are being charged only for transactions you made. Immediately report any irregularities.

12. Do not reply to any e-mail that requests your personal information.

Be very suspicious of any business or person who asks for your password, PIN (Personal Identification Number), or other highly sensitive information.

If you experience anything that arouses your suspicions, please intimate our call center representative or ENBDS Head office on the numbers given above.

Useful Facts on-

I. Phishing

Criminals use e-mails or links on web sites to lure victims onto fake Web sites. At these sites, the victims willingly enter their own credit card numbers, bank account numbers and other important information. This is called "phishing."

You probably think you will never fall for such a trick. However, these crooks are making you believing on their scam. Spoofed e-mail addresses and Web sites that look identical to financial institutions, Internet service providers, and other businesses are being used for this type of phishing. The recent phishing e-mails appear as if they came from well known Companies / Banks, replete with official logos, verbiage and links.

The government, police and banks are working together to combat this problem. But it's difficult to catch the crooks; many are overseas. The spoofed Web sites are active for a short time, and then they disappear.

Until this problem is eradicated, here are four steps to protect against the theft of your own personal information and your company's valuable business data.

Most phishing scams are sent through e-mail. By following these guidelines, you can help protect yourself from these tricky scams.

Do be wary of clicking on links in e-mail messages.

Links in phishing e-mail messages often take you directly to phony sites where you could unwittingly transmit personal or financial information to con artists. Avoid clicking on a link in an e-mail message unless you are sure of the destination. Even if the address bar displays the correct Web address, don't risk being fooled. There are several ways for con artists to display a fake URL in the address bar on your browser.

Do report suspicious e-mail.

If you suspect any phishing e-mail received which designed to steal your identity, report the e-mail to the faked or "spoofed" organization. Contact the concerned organization directly (not through the e-mail you received) and ask for confirmation. If you think that you have received a phishing e-mail message, do not respond to it.

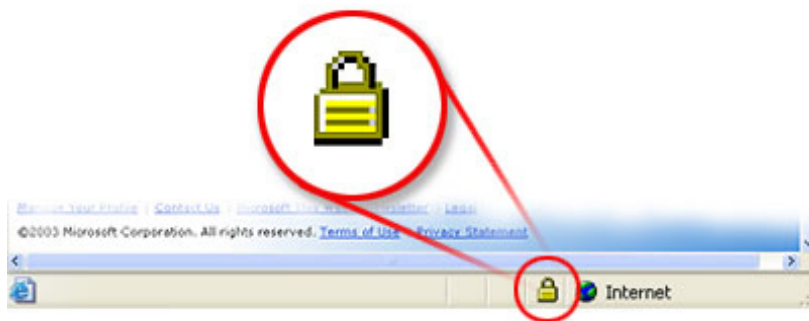
Do type addresses directly into your browser or use your personal bookmarks.

If you need to update your account information or change your password, visit the Web site by using your personal bookmark or by typing the URL directly into your browser.

Do check the security certificate when you are entering personal or financial information into a Web site.

Prior to you entering personal or financial information into a Web site, make sure the site is secure. In Internet Explorer, you can do this by checking the yellow lock icon on the status bar as shown in the following example.

Example of a secure site lock icon. If the lock is closed, then the site uses encryption.



The closed lock icon signifies that the Web site uses encryption to help protect any sensitive, personal information that you enter, such as your credit card number, Social Security number, or payment details. It's important to note that this symbol doesn't need to appear on every page of a site, only on those pages that request personal information. Unfortunately, even the lock symbol can be faked. To help increase your safety, double-click the lock icon to display the security certificate for the site. The name following 'issued to' should match the name of the site. If the name differs, you may be on a

fake site, also called a "spoofed" site. If you're not sure whether a certificate is legitimate, don't enter any personal information. Play it safe and leave.

Do not enter personal or financial information into pop-up windows. One common phishing technique is to launch a fake pop-up window when someone clicks on a link in a phishing e-mail message. To make the pop-up window look more convincing, it may be displayed over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information, because there is no way to check the security certificate. Close pop-up windows by clicking on the red X in the top right corner (a "cancel" button may not work, as you would expect).

II. Social Engineering

Definitions

Social engineering is the art and science of getting people to comply to your wishes" ("an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" or "getting needed information (for example, a password) from a person rather than breaking into a system"). In reality, social engineering can be any and all of these things, depending upon where you sit. The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this fact.

Target and Attack

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals. The Internet boom had its share of industrial engineering attacks in start-ups as well, but attacks generally focus on larger entities.

The Threat of Social Engineering and Your Defense against It

There are several methods that the malicious individual can use to try to breach the information security defenses of an organization. The human approach, often termed Social Engineering, is one of them.

Intruders and hackers are on the lookout for ways to gain access to valuable resources such as computer systems or corporate or personal information that can be used by them maliciously or for personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Often times, in fact more often than one can guess, they get through because of human behaviors such as trust – when people are too trusting of others, or ignorance – people who are ignorant about the consequences of being careless with information. Social Engineering uses human error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware. The ultimate security wall is the human being, and if that person is duped, the gates are wide open for the intruder to take control.

Categories of Social Engineering

There are two main categories under which all social engineering attempts could be classified – computer or technology based deception, and human based deception.

The technology-based approach is to deceive the user into believing that he is interacting with the ‘real’ computer system and get him to provide confidential information. For example, the user gets a popup window, informing him that the computer application has had a problem, and the user will need to reauthenticate in order to proceed. Once the user provides his id and password on that pop up window, the harm is done. The hacker who has created the popup now has the user’s id and password and can access the network and the computer system.

The human approach is done through deception, by taking advantage of the victim’s ignorance, and the natural human inclination to be helpful and liked. For example, the attacker impersonates a person with authority; He places a call to the help desk, and pretends to be a senior Manager, and says that he has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. At the very least, the individual can now access the Personnel systems as if he were the manager, and obtain the social Security numbers and other confidential/private information of several employees. He could of course do more damage to the network itself since he now has access to it.

Impact of Social Engineering on the organization:

Information Security is essential for any organization to continue to be in business. If information security is not given priority, especially in the current environment with the threat of terrorism looming in the background every day, even a small gap in security can bring an organization down.

The financial cost could be punitive to the organization and to the individual. So much so, those insurers are now beginning to cover losses arising out some kinds of security breaches.

Cyber attacks cost U.S. companies huge, according to a report released by the San Francisco-based Computer Security Firm and the San Francisco FBI Computer Intrusion Squad. The study found that 90% of 273 respondents detected some form of security breach in the past year. But this is probably an underreported figure. Less than half the companies in one survey were willing or able to quantify the loss.

Common techniques used in Social Engineering

(a) Direct approach

It is 3 pm on Sunday, and Employee A (Jack) is working on resolving a critical problem in the Personnel computer system, and is called away by an emergency at home. Employee B (Jill), who has been upset with his manager, offers to help out, and work on the problem. However Jill does not have access to the system, and there is no time to go through the proper channels to request the access for Jill. So Jack gives Jill his ID and password, without realizing that Jill has an ulterior motive in offering to help.

When Jack is sorting out his emergency situation, Jill has access to the network, the database and anything else that Jack has access to. Jill can now do what he wishes, and even better, he can do it without having his identity revealed in the process.

Or take the very common security problem of tailgating. Joe, who has forgotten his passkey into the building, shadows Barb as she ‘keys in’, and slips in after her. Often Barb does not know Joe, or even

notice that Joe has tailgated after her. And more often than not, even if Barb has noticed, she will not turn around and stop Joe from tailgating. She would not feel comfortable doing that, as it might create a scene in front of others. If Joe is an intruder, he has achieved the first step in his plan - he has gained physical access into the premises.

(b) Dumpster Diving

Whoever would have thought that throwing away junk mail or a routine company documents without shredding, could be a threat? But that is exactly what it could be, if the junk mail contained personal identification information, or credit card offers that a 'dumpster diver' could use in carrying out identity theft. The unsuspecting 'trash thrower' could give the Dumpster Diver his break.

Company phone books and organization charts provide phone numbers and locations of employees, especially management level employees who can be impersonated to the hacker's benefit.

Procedure and policy manuals can help the hacker to become knowledgeable about the company's policies and procedures, and thus be able to convince the victim about their authenticity.

Calendars are an important source of information about meetings; vacation etc, that the hacker can use to improve his 'storyline' when deceiving the unsuspecting secretary.