On-line security Decalogue

mBank.pl

Security measures adopted in CompanyNet system

Over the last few years the Internet has become a major source of threat to companies. The reason for this is the widespread access to this medium as well as the fact that the Internet has become a place where we live our everyday lives: socialize with friends, shop and bank. Viruses, attempted frauds or the so-called malicious software can materially affect the operation of a business. Although the purpose of the Internet is to make our lives easier, it is worth knowing the threats it poses and doing everything to protect your company from them.

1

Find out more about the security measures adopted in mBank CompanyNet system

The security rules published on mBank's official website must be scrupulously observed at all times. If you notice any irregularities or have doubts, do not hesitate to report them immediately to the support team dedicated to CompanyNet system users.

2

When logging into CompanyNet system, always use trusted computers known to you

Do not log into CompanyNet system using computers from outside your company network.

3

Update the anti-virus software, operating system and applications vital to its operation (Internet browsers, etc.) on a regular basis and scan your computer for viruses cyclically

Hackers are constantly looking for security holes in software, which they exploit to commit cyber-crimes.

The producers of operating systems and applications publish “patches” to remove vulnerabilities to attacks using such holes. Since an anti-virus monitor may not be as effective as a scanner activated on demand, you should regularly use anti-virus software to scan your computer.

4 Report to the Bank any untypical behaviour of CompanyNet system

If you notice untypical operation of the system (e.g. repeated incorrect logins, additional fields to enter password or erroneous authorisation of payments), immediately stop using the device showing the symptoms of a virus in action. Such behaviour of the system should be reported without delay to the Contact Centre - support team dedicated to Internet banking users.

5 Pay attention to the counterparty’s account number

When authorising orders, verify the counterparty’s account number. There are viruses capable of switching the counterparty’s account number in your browser’s memory.

6 Always confirm a change in the counterparty’s account number in a secure manner

If your counterparty or supervisor informed you by e-mail or phone about a change in account number, additionally confirm this information, e.g. on the phone or personally, to make sure that the information is accurate.

7 Do not open e-mails and e-mail attachments from unknown sources

Such attachments may introduce viruses or other malicious software to your computer which is difficult to detect by anti-virus software.

8 Avoid sites offering very attractive content or promising price bargains

Also websites offering “freeware” software can be extremely dangerous, as very often hackers add malicious code to them.

9 Do not open CompanyNet system by clicking links e-mailed to you

In order to log into the system, use only the system’s address given on mBank’s portal or use the direct address: https://CompanyNet.mBank.pl.

10 Never disclose your ID, alias or token to any third party

The ID assigned by mBank and the alias created by CompanyNet system user are confidential. In accordance with the agreement, the client, being their holder, is responsible for keeping these authorisation methods confidential.

What can make our systems even more secure?

FireWall

Firewall is one of the methods of protecting computers, networks and servers against intruders. Firewall can take the form of hardware with dedicated software or software alone and prevents unauthorised parties or programs from accessing our resources. Not more than several years ago firewall software was available and dedicated to key servers or large networks. However, along with the rapid technological development, firewall has become indispensable for any home computer connected to a local area network (LAN) or the Internet. Firewall installed on your home computer scans all outgoing and incoming network traffic and limits and prevents two-way access for unknown programs or users.

Anti-virus software

TIt is a software used to detect, protect against, fight and remove computer viruses and to repair the damage caused by viruses. If you run an application infected with malicious software, your anti-virus software acts in order to remove the virus and allow you to access the application. Frequent updates of virus definitions are crucial for every anti-virus software, as they allow you to keep your anti-virus program up to date with the "world of viruses". Updated definitions allow the program to gather information about the latest viruses and instructions on how to fight them and repair the damage they cause. Renowned producers of anti-virus software update virus definitions in their products on a daily basis.

Anti-spam software

Type of software used to block unsolicited e-mails. Anti-spam software filters e-mails and uses the so-called blacklists of addresses and domains used by spammers. Usually anti-spam software allows you to set your own rules which can then be modified or defined, e.g. keywords used in advertising materials, and thus blocks your mailbox to e-mails containing these words in the subject line. However, anti-spam software programs are not flawless and may sometimes block e-mails that in fact should be delivered.

The most common threats on the Internet

Increasingly often the media report that hackers impersonate counterparties or supervisors of people working in banking systems. By launching social engineering attacks, they try to induce them to execute unscheduled or scheduled payments to fake counterparty's accounts provided by e-mail or on the phone. That is why every change in the account

number should be additionally confirmed via a channel other than that used to convey the original message.
Other frequent threat involves hackers fraudulently obtaining personal data such as user's password, ID, alias or credit card details. This type of attack employs social engineering techniques. Nowadays, cyber-criminals tend to use phishing techniques to make money. Often, Internet banks or on-line auction sites fall victim to their attacks. Phishers usually send spam to a large number of potential victims directing them to a fake website which looks almost identical to an Internet bank; this way they trick unsuspecting victims into divulging information. Typically, they send information about alleged account deactivation and inform clients that an activation using their confidential data is necessary. Often they use a fake website pretending to be an Internet bank's website on which the users enter all their log in details. The clients are unable to log in, but their data are compromised by phishers.

Spam

Spam are unsolicited messages sent by e-mail. Usually it is sent on a mass scale. The idea behind spam is to send high volumes of identical commercial information to unknown recipients. The content of spam messages is of no importance. Spam could be compared with fliers left on our doorsteps or attached to letters. In the majority of cases spam is used for commercial purposes and takes the form of e-mails encouraging the recipients to buy advertised goods or luring them by a prospect of winning a trip. Sometimes, however, spam is used by hackers who, by impersonating a bank or another institution, try to trick us into divulging confidential information or installing software that carries viruses and spyware.

Viruses

A computer virus is a self-replicating segment of executable computer code embedded within a host program or linked to it. In order to act, a virus needs a host in the form of a computer program. When the host program is started, usually the malicious code of the virus runs first followed by the program.

After successfully infecting the computer, further action of the virus depends on its type and results in:

- hackers fraudulently obtaining data allowing them to make payments in on-line banking
- replication within the infected system
- infection spreading to new files being opened or created
- deletion or damage of data in systems and files
- wasting system resources without damaging them

In terms of virus types, viruses can be divided into:

- boot sector viruses - target the boot sector of floppy discs and hard drives
- file viruses - target the executable files of an operating system
- BIOS viruses - harmful to computer's BIOS (type of firmware responsible for correct configuration and system start-up)
- macro viruses - embedded in non-executable files, e.g. Word or Excel files, used to launch the attack; the infection spreads using macros contained in these documents
- mobile viruses - increasingly frequent; mobile viruses are becoming a real threat due to the development of software dedicated to mobile phones

mBank S.A. ul. Senatorska 18, 00-950 Warsaw, Poland
phone 22 829 00 00, fax 22 829 00 33
msp-korporacje@mBank.pl