

Online Security for eBanking

Electronic Banking

Bank Leumi USA offers electronic online banking through the Internet. We provide a full range of online banking services for our customers. We implement the highest standards and state of the art security measures to keep your electronic banking information and transactions safe and secure. Nonetheless, the security of electronic banking is a two-way street between us and our customers. The following information is provided as a means to enhance your awareness of the security of your electronic banking environment and provide insight as to what you can do to protect your own information.

Preparing for your eBanking experience

The computer you use to connect to Bank Leumi eBanking services could be the weakest link in the security chain. To ensure the security of your ebanking sessions be sure to have reputable anti-malware software installed, that its virus detection patterns are up to date (a daily event) and that you install all the security patches made available by software vendors like Microsoft, Adobe Reader and Flash, Oracle Java, Apple Quicktime.

When you pick a password

As you well know, passwords serve to help authentication you to our ebanking application. As such, be sure to select a password that is hard to guess, keeping in mind that a computer program may be doing the guessing.

We encourage you to use a "complex" password that has at least length of 7 characters and is composed of multiple character sets (uppercase letters, lowercase letters, numbers, and special characters). You should change your password at least twice per year and do not use the same password for multiple online accounts.

When you select security questions

You should be very interested in the set of "challenge questions" you select for our site and any other site that uses this technique of user authentication. Every website intends to be easy for its customers to use, so the challenge questions they utilize will tend to be easy to guess, or to lookup. And in the age of social network sites like Facebook, Twitter, Google+ and LinkedIn, challenge questions have become considerably easier to guess.

When you pick and respond to your challenge questions, be sure you are not revealing the answer in some other place where it can be found and used against you.

During your relationship with us

Did we say that you should keep your anti-virus software and detection patterns up to date? We'd like to remind you that we will not contact you by email to inform you of a problem with your account. Be on guard against email containing hyperlinks that request you to login to fix a problem...

You are under attack

Whenever you connect to the Internet and "browse the web" or enjoy the convenience of email, you should know that you are under attack. Simply by connecting to the Internet you are making yourself a potential target of criminals. Everyday, criminals use automated tools to scan for unprotected or vulnerable computers. Criminals may target you specifically or you may be the subject of a random attack. What ever the case, there are two main ways by which your computer can be affected by cyber crime:

Your computer is used to steal your personal information: Two examples are trojans and spyware. Trojans are a form of malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer. A Trojan may be used to install spyware such as keylogging; software, which records keystrokes including passwords and then sends the captured information to the attacker.

Your computer is used to facilitate other crimes and attacks on others: Computers can be hijacked to provide storage of illegal images or illegal downloads of music. Hijacked computers could also be used as a platform to launch attacks or commit crimes against others.

Information, whether personal or business related, is becoming increasingly valuable to criminals. Where personal information, such as bank account, credit card, or social security numbers, is stored, whether on your personal computer or with a trusted third party such as a bank, retailer or government agency, a cyber criminal can attempt to steal that information which could be used for identity theft, credit card fraud or fraudulent withdrawals from a bank account.

The attackers are trying to prey on anyone they can reach via any method. As their malware spreads, they gain control of an increasing number of Internet-connected computers - some of which you may end up visiting. When you do, the breached site will try to download malicious software to your computer. This is known in the business as a "drive-by" attack; all you need to do is visit the breached site with an unprotected computer and you will fall victim too.

- Be wary of using computers you do not own, like those at Internet Cafes
- Be selective in the websites you choose to visit
- Attackers work to have their malicious websites listed at the top of Google searches

Phishing

Phishing (fishing) is a form of Social Engineering. The attacker casts a net of fraudulent emails in the expectation that some people will let down their guard and follow the instructions those emails contain. Typically, these emails will claim that the sky is falling and you must take action immediately! When a victim falls for a phishing email, they become involved in cyber tricks that work to plant trojans and spyware on their computer. If successful, the attackers will work to have their activities remain undetected, while they steal login credentials and other private data, and send it back to the attacker.

Spear Phishing

Spear phishing is specialized form of phishing. In this category, the attacker has taken time to identify their targets and perform background research on them. The attackers then use this information to craft targeted emails that will be more convincing to the intended victim. This form of attack is growing in prevalence at a dramatic rate.

SMiShing

Fraudsters are using the popular Short Message Service (SMS messaging, otherwise known as "texting") to target victims. This is frequently called smishing. Victims receive "texts" (SMS messages) claiming to be from their bank stating that the sky is falling (or some other pretense), and you'd better act now by contacting a phone number or website, where they disclose their personal information.

Vishing

More and more, voice communication is being conducted over computer data networks. This is commonly referred to as Voice over Internet Protocol, or VoIP. Vishing is phishing, using the VoIP technology.

People have come to trust their telephones over the years. They typically trust that what is displayed on the caller ID is a fact. This is not the case, however. An attacker can use specialized tools to define the caller ID data they want to have displayed and, in doing so, attempt to attack phone's owner either directly or via voicemail.

Keyloggers, Trojans & Spyware - Oh My!

Once an attacker has "hooked" you into their scheme using any form of phishing, or if they catch you when you happen to browse to a web server that they have already breached and infected, they work to breach your PC and implant keyloggers, trojans and other malware, in order to steal from you all that they can.

Antivirus solutions help to provide protection against these techniques, but they are not perfect. If you believe your PC has already been infected, you should consult your anti-virus vendor for case-by-case support. Until the issue is resolved, you should refrain from using the suspect PC to access websites that require login credentials, such as

your ebanking account. You should also notify your account representative, so that we can apply extra monitoring for your account.

SmartPhones and Tablets

Modern "smartphones" and "tablets" are powerful computers, just like laptops and desktops. Some smartphones today are as powerful as servers were when the Internet was first being formed. These devices are coming under increasing attack by cyber-thieves. We have already discussed how voicemail can be tricked into believing a fraudster is in fact you! You need to consider this and be sure to set good passwords to guard your voicemail.

The discovery of vulnerabilities in Apple IOS, Google Android and Windows Mobile are published regularly. Attackers will attempt to exploit these vulnerabilities any way that they can, often via vishing and smishing. Additionally, attackers rely on users to install apps that appear to be slick. They will post malicious apps that look like legitimate apps in the hopes that people will download and install them. They will also post malicious mobile apps in the banner ads on websites that have already been breached. Finally, a tried and true method of hacking is to publish apps that claim to be for "security", but in reality are the malicious code we all want to defend against.

We encourage iPhone and Android owners to obtain their applications only from the Apple App Store or the Android Market. You should install antivirus and browser protection as soon as possible, and keep it up to date. This increases the likelihood that there is no malicious code in the apps that you choose to run.

We won't

We will not send you email that requests you to 'click a link' to confirm or correct your information with us. This is a trick fraudsters use in order to steal your user credentials. Fraudsters will try to convince you that your account with us is in jeopardy and you need to act immediately. Be aware of their attempts; resist acting upon them.

We recommend

The best way to protect yourself from cyber crime is to use common sense, be prepared and take precautions.

- Keep your operating system updated/patched; set it to "auto update". For more information: (Windows) <http://windows.microsoft.com/en-US/windows/help/windows-update> or (MacOS) <http://support.apple.com/kb/ht1338>
- Use anti-virus and anti-spyware software and keep your subscriptions up-to-date.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted. For more information: (Internet Explorer) <http://windows.microsoft.com/en-US/windows7/How-to-know-if-an-online-transaction-is-secure>, or (Firefox) http://www.mozilla.org/security/#Tips_for_secure_browsing.
- Be cautious about all communications you receive including those purported to be from "trusted entities" and be careful when clicking links contained within those messages.
- Do not respond to any unsolicited (spam) incoming e-mails.
- Do not open any attachments contained in suspicious emails.
- Do not respond to an email requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- Beware of emails that threaten any dire consequences should you not "verify your information".
- Do not enter personal information in any window that "pops up" when you are browsing a Web site. Providing such information may compromise your identity and increase the odds of identity theft.
- Have separate passwords for work related and non-work related accounts.

For the Extra Security Conscious

The Financial Services Information Sharing and Analysis Center (FS ISAC) recommends to eBanking customers the use of an isolated, dedicated computer for transacting your banking needs. If you would like more details on this approach, please notify your Relationship Manager and we'll make arrangements to work with you, to ensure you understand the details and what is involved.

Important Online Resources

Bureau of Consumer Protection: <http://www.business.ftc.gov/privacy-and-security>

The FTC's Bureau of Consumer Protection enforces laws that protect consumers against unfair or deceptive practices. The Business Center gives you and your business tools to understand and comply with the law.

FTC Identity Theft Site: <http://ftc.gov/bcp/edu/microsites/idtheft/>

Microsoft Security: <http://www.microsoft.com/security>

Guidance for creating passwords: <http://www.microsoft.com/security/online-privacy/passwords-create.aspx>

MITRE - Common Vulnerabilities: <http://cve.mitre.org/>

The CVE is a dictionary of publicly known information security vulnerabilities and exposures.

Multi-State Information Sharing & Analysis Center (MS-ISAC): <http://msisac.org/daily-tips/Surf-Safe-on-the-Internet.cfm>

Cyber Tips Newsletter – Surf Safe On The Internet

National Consumer Protection Week: <http://www.ncpw.gov/>

National Cyber Security Alliance: <http://staysafeonline.org/in-the-home/protect-yourself>

OnGuard Online: <http://www.onguardonline.gov/default.aspx>

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you guard against internet fraud, secure your computer, and protect your personal information.

SANS Ouch! Newsletter: <http://www.securingthehuman.org/resources/newsletters/ouch>

US-CERT Shopping Safely Online: <http://us-cert.gov/cas/tips/ST07-001.html>

The Virus Bulletin newsletter: <http://www.virusbtn.com>

Glossary

Identity Fraud - the use of your personal information, including bank or credit card account number, or other identifying information without your knowledge to commit fraud or deception

Keylogger - specialized software that records keystroke activity on your PC. Malicious keyloggers have been coded to identify when a victim browses to a sensitive website (banking sites and sites that require authentication), at which point it wakes up and records what you type as you input your username and password. This data is then often encrypted and relayed back to the attacker for further use.

Malware - software designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.

Social Engineering - techniques used to manipulate people into performing actions or divulging confidential information. The term typically applies to trickery used for information gathering or computer system access. In most cases the attacker never comes face-to-face with the victim.

Trojan Software - software that is represented as being good and useful that contains malicious code that tries to steal your private banking information and forward it to the thieves.