Luther Burbank®

Savings

Online Banking
Customer Awareness and Education Program

Member FDIC

Table of Contents

Online Banking Customer Awareness and Education Program Overview

The purpose of the Luther Burbank Savings ("the Bank" or "LBS") Online Banking Customer Awareness and Education Program ("the Program") is to educate our customers of the risks associated with online banking and what safeguards to follow. The Program highlights the importance of online banking security measures that can protect online banking customers from being victims of fraud. Specifically, the Program addresses email security, password security, computer and Internet security, social engineering threats, unsolicited contact, and regulatory laws related to electronic funds transfers. LBS strongly believes that public awareness of online banking risks and how to avoid them is the strongest weapon in the defense against monetary losses.

Unsolicited Contact

Remember that LBS will never make or send **unsolicited** calls, texts or emails asking customers to provide passwords, login IDs, security codes, PINs or account information such as Social Security number, Account Number, Debit Card Number, or other personal information.

LBS will only contact our customers regarding online banking activity on an unsolicited basis for the following reasons:

- To confirm suspected fraudulent activity;
- To notify you of a potential disruption in service; or
- To confirm changes submitted to your online banking profile.

If you receive an unsolicited contact from an LBS employee for any reason not cited above, your identity will be confirmed through a series of security questions and you will always have the option of hanging up and calling LBS directly to confirm the validity of our request. Remember, LBS will **never** ask for your logon security credentials (passwords, login IDs, security codes, PINs).

Luther Burbank Savings Contact Information

You are protected in a variety of ways when you use online banking; however, it is important to contact us (LBS) in the event your online access has been compromised. You should also report any unauthorized, suspicious or unexpected transactions immediately.

To report suspicious activity on any of your account(s), or if you have questions about the security of your account(s), you can call us at: **844-269-1031** or email us at fraud@lbsavings.com. You can also dial our Interactive Voice Response (IVR) system at **800-969-8386**, Option 1 then Option 5. The security of your money and information is as important to us as it is to you. Let's work together to protect it.

Online Banking Security Certification

LBS requires that customers with access to "high-risk online banking transactions" perform a risk assessment and controls evaluation on an annual basis. As a result, LBS requires that all customers with access to either Wire Manager, ACH Manager, or Remote Deposit Capture (RDC) complete a risk assessment questionnaire via the **Online Banking Security Certification** annually. The Online Banking Security Certification evaluates your controls over your online banking practices. Failure to complete the certification could result in the suspension of online banking services. For business online banking customers who do not have access to conduct these high-risk transactions, LBS encourages you to also complete the **Online Banking Security Certification** to ensure that existing online banking safeguards are evaluated periodically. You can obtain the **Online Banking Security Certification** by contacting LBS at **888-578-4495** or email us at cashmgmt@lbsavings.com.

Email Security

Malicious Emails

Malicious emails, also known as Phishing, is when a fraudulent email is sent by a fraudster where they are attempting to trick the recipient into providing sensitive personal information such as an account number, password, username or Social Security number. The malicious email can also be a trick that instructs you to change wire instructions to a different beneficiary.

Email Attachments

The malicious email may also contain a link or attachment that, if clicked or opened, will load malware onto your computer. Malware is a type of malicious software that is designed to collect sensitive financial and personal information. This is called "pharming". This can lead to identity theft or unauthorized access to online banking accounts. Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- Email is easily circulated. Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email — they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.
- Email programs try to address all users' needs. Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.
- Email programs offer many "user-friendly" features. Some email programs even offer the option to automatically download email attachments, which immediately exposes your computer to any viruses within those attachments.

Following are a few tips on what to look out for when it comes to email attachments:

- Attackers often try to hide malicious files in email archives, such as zip files. As a result, be extra cautious with attachments that have .zip, .zipx, .rar, .7z file extensions.
- Newer Microsoft Office files extension are .docx, .xlsx, and .pptx for Word, Excel and PowerPoint documents. The same documents with macros can be potentially dangerous and end with "m" – .docm, .xlsm, and .pptm. So please watch out for extensions ending in "m".
- Files with double extensions are also suspicious. Remember, the only extension that matters is the last one. For example, a normal Microsoft Word document file name may be "example.docx"; however an attacker will manipulate the file name by adding a second extension to make it look legitimate but the document is actually a malicious executable file that will look like this → example.docx.exe
- It is important to not trust attachments from someone you don't know.

Verify Emails

If you receive an email that is unexpected, too good to be true, or contains suspicious web-links or attachments, you should do the following:

1. Verify the validity of the email through a phone call.
2. If the email is not valid, delete the email immediately.
3. Contact the true sender, if possible, and inform them that a fraudulent email was sent from their email account.

Strong and Complex Email Passwords

Personal email accounts are an important part of your online activity. Email accounts are used to register for online services, online banking, and social media. It's important that strong and complex passwords are used to protect these email accounts. The next section will provide an overview on how to create strong and complex passwords.

Password Security

Password Secrecy

Passwords should not be shared, and should be stored in a secure way. Passwords should not be transmitted unencrypted. For example, passwords should not be sent via unencrypted email. Also, passwords should not be re-used. For example, your online banking password should not be the same as your email password.

Password Length and Composition
Password length and composition determines the complexity of a password. The complexity of a password should increase depending on the value or sensitivity of the asset being protected. Common identifiers such as Social Security numbers, phone numbers, names, addresses or dictionary words should not be used as a password. Complexity is gained through a longer password with more characters; using numbers and letters; using upper and lower case; and special characters.

How to create a strong, complex password:

1. Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, movie, song lyric, or quotation you like. Example: **"I Want To Put A Dent In The Universe"**
2. Remove all but the first letter of each word in your phrase: **IWTPADITU**
3. Replace several of the upper-case letters with lowercase ones, at random: **iWtpADitU**
4. Now substitute a number for at least one of the letters. (Here, we've changed the capital "I" to the numeral 1: **iWtpAD1tU**
5. Finally, use special characters ($, &, +, !, @) to replace a letter or two -- preferably a letter that is repeated in the phrase. You can also add an extra character to the mix. (Here, we've replaced the "t" with "+", and added an exclamation point at the end: **iW+pAD1tU!**)

Computer and Internet Security

Anti-Virus
All computers that are used by you to perform any financial or online banking transactions should have up-to-date anti-virus software installed. This software protects the computer from malware that is designed to steal personal and financial information that leads to identity theft and fraudulent transactions.

Firewall
A firewall protects a computer from outside attacks by shielding it from malicious and unnecessary internet traffic. Remember to keep your computer's operating system up to date, and your firewall turned on.

Security and Application Patches
Operating systems, such as Windows, need regular updates that fix problems or mitigate vulnerabilities. These are called "patches". The most critical patches are called "security patches". Individual applications or software on a computer may also require patches. These applications include Microsoft Office, web browsers, JAVA, and Adobe Acrobat. You should ensure that any computer that is used to perform financial or online banking transactions is patched as the patches are made available by the software vendor.

Internet Browsing
While "surfing" the Internet, follow these steps to protect your computer from the majority of Internet crime:

- If you download anything from the Internet such as music, movies, or pictures, make sure you do so only from trusted websites. Downloads can be infected with spyware/adware attached to the file.
- Watch for signs of spyware—frequent pop-up ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection. The pop-up ads (adware) sometimes appear to offer free credit reports or credit scores as part of the scam. Run a full system anti-virus and anti-spyware scan to identify and safely remove spyware.
- Do not use public computers to perform any type of online banking transactions. Just logging on to online banking may give away passwords and other private information if spyware has been installed on that computer.

Spoofed Websites
Cybercriminals may set up fake websites that appear to look like Luther Burbank Savings' website in an attempt to obtain your login credentials. When accessing Luther Burbank Savings' website, verify its authenticity by looking for the following URLs:
www.lutherburbanksavings.com/
www.lutherburbanksavings.com/log-in/

Mobile Banking Unauthorized Apps
Cybercriminals may create fake websites offering a bank's app for download. Do not attempt to download apps from non-trusted sources as they may contain malware or attempt to trick you into providing personal or account information.

Important: The Luther Burbank Savings mobile banking app is only available for download through the Google Play and App Store.

Vishing and SMiShing
Scam phone calls, also known as **Vishing**, is a social engineering tactic used by Cybercriminals. During a Vishing attack, a Cybercriminal may use a fake caller ID to pose as a representative of LBS, a trusted person or entity you regularly work with. They will then attempt to scam you into providing personal account information over the phone or may ask you to change routing information for electronic funds transfer activity. If you receive such a call, hang up and call LBS using a known number.

Phishing texts, also known as **SMiShing**, may claim to be from your bank and include urgent requests or warnings that your account is about to be closed or has been locked/deactivated. These messages may ask you to call a number, visit a website or respond by text with your personal or account information. If you receive a suspicious text that asks for personal information or login information, do not respond and contact LBS using a known number and report the text message.

Important: LBS will never ask for login credentials, personal or account information by email or text.

Trusteer Rapport
Luther Burbank Savings' online banking service includes several security features to give you peace of mind anytime and anywhere you manage your money. Add an extra layer of defense against the most common types of cyber fraud by downloading IBM Trusteer Rapport, free of charge, and further safeguard your online banking experience.

Trusteer Rapport works alongside your current anti-virus software to increase your protection against cyber fraud while you access your online banking account. The software detects and removes banking malware to secure your online banking session. It also prevents attempts to redirect you to fraudulent banking websites. Trusteer Rapport downloads in minutes. Once installed, the software automatically runs in your computer's background to verify that you are connected to the Bank's actual website, creating a secure line of communication.

To keep your personal information secure, download Trusteer Rapport for free to either your PC or Mac by visiting our website at:

https://www.lutherburbanksavings.com/banking-resources/ibm-trusteer-rapport/

Disposal of Information

Paper documents that contain sensitive personal or financial information should be shredded by a cross-cut before disposal or recycling. Documents containing the following information should always be shredded:

- Names
- Addresses
- Phone numbers
- Email addresses
- Account numbers
- Birth dates
- Passwords, login IDs, security codes, or PINs
- Signatures
- Social Security numbers

The following documents may contain the information listed above, if so these documents should be shredded.

- Address labels
- Bank statements, ATM receipts, and canceled or voided checks
- Bank
- Birth certificate copies
- Credit reports
- Employee pay stubs
- Expired credit cards
- Legal documents
- Insurance documents
- Investment, stock and property transactions
- Medical records
- Pre-approved credit card applications
- Resumes
- Tax forms and transcripts
- Travel itineraries and used airline tickets
- Utility bills

Identity Theft

Identity theft is when someone uses your personal or financial information without your permission. They might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers. And they could use them to:

- Buy things with your credit cards
- Get new credit cards in your name
- Open a phone, electricity, or gas account in your name
- Steal your tax refund
- Use your health insurance to get medical care
- Pretend to be you if they are arrested

Taking steps to protect your personal information can help you avoid identity theft. Here's what you can do to stay ahead of identity thieves.

- Never give your personal information, passwords, login IDs, security codes, PINs or account information to someone who calls, emails, or texts you.
- Protect documents that have your personal information.
- Report lost or stolen checks or credit cards immediately.
- Shred all documentation that contains confidential information (i.e. bank and credit card statements, bills and invoices that contain personal information, expired credit cards and pay-stubs).
- Check your credit report annually.

If you are a victim of identity theft, perform these steps immediately:

- Call the companies where you know fraud occurred. Ask to freeze accounts and change logins, passwords and PINs for your accounts where possible.
- Contact the three credit bureaus and place a free one-year fraud alert. Also, obtain a copy of your credit reports.
- Report the identity theft to the Federal Trade Commission (FTC) by completing an online form at https://www.identitytheft.gov/Assistant or by calling 1-877-438-4338. Include as many details as possible.
- File a report with your local police department. Provide them with a copy of your FTC Identity Theft Report, your government issued ID with photo, proof of your address, and other proof of the theft. Make sure you obtain a copy of the police report.

Credit Reports

Any consumer can request one free copy of their credit report per year from each of the three major credit reporting companies. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Contact the three major credit companies to request copies of your credit report:

Equifax
1-800-685-1111
PO Box 740241, Atlanta, GA 30374
www.equifax.com

Experian
1-888-397-3742
PO Box 2002, Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
PO Box 2000, Chester, PA 19022
www.transunion.com

Ransomware Risk

Ransomware is a form of malware used by cyber criminals to freeze your computer or mobile device, steal your data and demand that a "ransom" — typically anywhere from a hundreds to millions of dollars — be paid.

Ransomware Prevention for Consumers

- Don't click. Visiting unsafe, suspicious or fake websites can lead to the intrusion of malware. Be cautious when opening emails or attachments you don't recognize even if the message comes from someone in your contact list.
- Always back up your files. By maintaining offline copies of your personal information, ransomware scams will have a limited impact on you. If targeted, you will be less inclined to take heed to threats posed by cyber criminals.
- Keep your computers and mobile devices up to date. Having the latest security software, web browser and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
- Enable popup blockers. To prevent popups, turn on popup blockers to avert unwanted ads, popups or browser malware from constantly appearing on your computer screen.

Ransomware Prevention for Businesses

- Educate your employees. Employees can serve as a first line of defense to combat online threats and can actively help stop malware from infiltrating the organization's system. A strong security program paired with employee education about the warning signs, safe practices, and responses aid tremendously in preventing these threats.
- Limit the use of privileged accounts as an effective way to stop lateral movement by attackers, thereby helping block the progression of an attack.
- Restrict users' ability to install and run software applications on network devices, in an effort to limit your networks exposure to malware.
- Employ a data backup and recovery plan for all critical information. Backups are essential for lessening the impact of potential malware threats. Store the data in a separate device or offline in order to access it in the event of a ransomware attack.
- Make sure all business devices are up to date. Ensure anti-virus and anti-malware solutions are set to automatically update and conduct regular scans so that your operating systems operate efficiently.
- Contact your local FBI field office immediately to report a ransomware event and request assistance. Visit https://www.fbi.gov/contact-us/field to locate the office nearest you.

Business Email Compromise (BEC) Risk

What is Business Email Compromise?
A type of phishing scheme, business email compromise (BEC) is a common form of cyber fraud where Cybercriminals employ social engineering techniques to manipulate victims by impersonating a trusted source and attempting to trick a victim into transferring money or sensitive data.

Cybercriminals typically avoid email security filters by not sending mass emails; instead, they target specific recipients, typically employees who perform regular wire transfers. They may even follow up with a phone call or perform other methods of authentication. As these communications appear to be from a legitimate source, BEC can be extremely difficult to recognize and can often go undetected.

Defending Against BEC
If you are involved in submitting a wire transfer in any way, whether it is for personal reasons (e.g. buying a house, escrow, etc.) or business related (e.g. paying a vendor, payroll, etc.) and you receive an email requesting that you create a new wire or change wire instructions to an existing wire, proceed with caution and keep the following in mind:

- Be skeptical of the request, especially if there is urgency in the language within the email.
- Review email addresses carefully to ensure that the correct domain appears.
- Even if you have been corresponding with an individual via email and they provide new or updated wire instructions, ALWAYS verbally verify the request, either in person or by phone to a known number.

Typical Methods of BEC Attack
Email Account Takeover Scenario: A Cybercriminal steals the email login credentials of one of your trusted business partners (ex. an escrow agent, colleague, supervisor, financial institution, and vendor) and sends fraudulent emails requesting confidential information or providing wire instructions.

Important: Even if the email appears to have been sent by a trusted person, business partner or someone within your organization, it may not be legitimate.

Impersonation Scenario: A Cybercriminal sends an email which appears to be from one of your trusted business partners with a legitimate request. The Cybercriminal may either use a spoof email (an email message with a forged sender address) or create a sender address that appears similar to that of your business partner. For example:

Real email address: jsmith@lbsavings.com
Fake email address: jsmith@lbssavings.com

Important: Cybercriminals may also copy electronic signatures and logos in their emails to appear credible.

BEC Cybercriminals are Savvy
Cybercriminals performing BEC attacks often make last-minute change requests to existing wires in hopes that they will not be detected prior to transfer. They will typically instruct victims to act quickly or in confidence when transferring funds.

BEC Cybercriminals are known to perform extensive research to make their emails appear more credible. They often use social media sites, such as LinkedIn, to gather names, titles and other relevant information about you, your financial transactions (you may have posted on social media that you're buying a house) or your company. Always be skeptical of wire instructions provided by email, and always verify verbally via a known number!

Corporate Account Takeover (CATO) Risk

During a corporate account takeover (CATO), Cybercriminals use your stolen business banking account login information (ex. user name, password) to initiate fraudulent wire or ACH transactions. Cybercriminals may use phishing emails, phone calls or social media networks to gain access to your account; or they may infect your computer or mobile device with malware to record login information. Visiting a fraudulent website or clicking an infected link or attachment from an email may compromise your computer.

To protect yourself and your organization from corporate account takeover attacks, perform the following:

- Do not click links or attachments in unsolicited emails. If you receive a suspicious email appearing to be from LBS, call us using a known number to confirm if the email is legitimate.
- Never click on pop-ups that claim your computer is infected and that offer software to scan and fix the issue.

Enhance the security of your computers and network by performing the following:

- Restrict use of computers dedicated to online banking and payments (no general web browsing, email or social networking).
- Never leave computers with administrative privileges and/or online banking access unattended − always lock or shut them down.
- Install and maintain spam filters, anti-virus and anti-spyware software; and block pop-ups.
- Install the latest security updates to operating systems and applications.
- Keep operating systems, browsers, software and hardware up-to-date.
- Back up files regularly and encrypt sensitive folders.
- Do not use public internet access when banking online.
- Watch for virus alerts and anti-virus software expiration notices.
- Keep up-to-date on the latest cyber security threats and news.
- Monitor bank accounts daily to detect unauthorized activity.
- Use multi-factor authentication where available to block unauthorized access attempts.

If you bank with LBS as a business, ensure that employees with access to online banking are trained on how to report suspicious activity to Luther Burbank Savings. We may assist with the following:

- Disabling online account access
- Changing the account password
- Opening new account(s), if needed
- Confirming if anyone has recently: added new payees; requested an address or phone number change; created new user accounts; changed access to existing user accounts; changed existing wire/ACH templates; changed the PIN; or ordered new cards, checks or other account documents to be sent to an unauthorized address.

Signs of a Possible CATO Attack

- Unusual activity on your business banking account
- Dramatic loss of computer/internet speed
- Unusual appearance of the online banking site or pop-up messages
- Unexpected rebooting or inability to shut down/restart your computer
- Sudden locking of your computer while in use
- Unexpected requests for your login IDs or PIN/password during an online banking session
- Unsolicited phone calls requesting your login IDs or PIN/password

Responding to a CATO Attack

- Immediately cease all online activity and remove any computers from the network that may be compromised.
- Submit a report to law enforcement (local police department) and the FBI via the IC3 portal at https://www.ic3.gov/.

Contact Luther Burbank Savings immediately if you believe you have been the victim of a CATO attack; if your login information and/or account number have been compromised; or if you notice any unauthorized activity on your account. Call **888-578-4495** or contact your branch directly.

Electronic Funds Transfers (Regulation E)

The Electronic Fund Transfer Act, also known as Regulation E, is designed to protect individual **consumers** making electronic fund transfers. The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's asset account.

The Electronic Fund Transfer Act establishes the basic rights, liabilities, and responsibilities of consumers who use EFT services. The following describes some examples of what is covered and not covered under Regulation E:

What is covered?	What is not covered?

Any transfer of funds that are initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to:
• Point-of-sale transfers;
• Automated teller machine transfers;
• Direct deposits or withdrawals of funds;
• Transfers initiated by telephone;
• Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal;
• Electronic check conversion, whereby you may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills; and
• Electronic returned check charge, whereby you authorize a merchant or other payee to initiate an electronic fund transfer to collect a charge in the event a check is returned for insufficient funds.
	• Checks;
	• Check guarantee or authorization;
	• Wire or other similar transfers through Fedwire;
	• Securities and commodities transfers;
	• Automatic transfers by account-holding institutions;
	• Any preauthorized transfer to or from an account if the assets of the account holding financial institution were $100 million or less on the preceding December 31; and
	• Telephone-initiated transfers. Any transfer of funds that:
	  • Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
	  • Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.

Important: Regulation E requires disclosure of the terms and conditions of EFT services and is provided by Luther Burbank Savings at the time of account opening.