
# Business/Commercial Client

# Internet Banking Awareness and Education Program

1.855.860.5952 TMClientSupport@opusbank.com www.opusbank.com

Rev. 012014

# Table of Contents

# Business/Commercial Client Internet Banking Awareness and Education Program

## Unsolicited Client Contact

Opus Bank will never contact its clients on an unsolicited basis to request their security logon credentials such as the combination of the client's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at **(855) 678-7226** or e-mail us at fraudunit@opusbank.com to report any activity of this nature.

Opus Bank will only contact its clients regarding online banking activity on an unsolicited basis for the following reasons:

- Suspected fraudulent activity on your account;
- Inactive/dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted to your online banking profile.

If you receive an unsolicited contact from an Opus Bank team member 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 Opus Bank to confirm that validity of our request. Remember, Opus Bank will NEVER ask for your logon security credentials.

## Self-Assessment

Online Banking Business/Commercial clients are strongly encouraged to perform an annual Self-Assessment focusing on their online banking practices and network security. A Self-Assessment will evaluate whether the client has implemented sound business practices to address the five key principles outlined in the "Securing Your Business" section within this document.

## Securing Your Business

Is your company keeping information secure?

Are you taking steps to protect sensitive information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

- **Take stock**. Know the nature and scope of the sensitive information contained in your files and on your computers.
- **Scale down**. Keep only what you need for your business.
- **Lock it.** Protect the information in your care.
- **Pitch it**. Properly dispose of what you no longer need.
- **Plan ahead**. Create a plan to respond to security incidents.

# Business/Commercial Client Internet Banking Awareness and Education Program

The following information is provided by the Federal Trade Commission, Bureau of Consumer Protection.

## Take Stock

Know the nature and scope of the sensitive information contained in your files and on your computers.

- Take inventory of all file storage and electronic equipment. Where does your company store sensitive data?
- Talk with your employees and outside service providers to determine who sends sensitive information to your business, and how it is sent.
- Consider all of the methods with which you collect sensitive information from customers, and what kind of information you collect.
- Review where you keep the information you collect, and who has access to it.

## Scale Down

Keep only what you need for your business.

- Use Social Security numbers only for required and lawful purposes. Don't use SSNs as employee identifiers or customer locators.
- Keep customer credit card information only if you have a business need for it.
- Review the forms you use to gather data — like credit applications and fill-in-the-blank web screens for potential customers — and revise them to eliminate requests for information you don't need.
- Change the default settings on your software that reads customers' credit cards. Don't keep information you don't need.
- Truncate the account information on any electronically printed credit and debit card receipts that you give your customers. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.
- Develop a written records retention policy, especially if you must keep information for business reasons or to comply with the law.

## Lock It

Protect the information that you keep.

- Put documents and other materials containing sensitive information in a locked room or file cabinet.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers.

- Require employees to use strong passwords.
- Caution employees against transmitting personal information via e-mail.
- Create security policies for laptops used both within your office, and while traveling.
- Use a firewall to protect your computers and your network.
- Set “access controls” to allow only trusted employees with a legitimate business need to access the network.
- Monitor incoming Internet traffic for signs of security breaches.
- Check references and do background checks before hiring employees who will have access to sensitive data.
- Create procedures to ensure workers who leave your organization no longer have access to sensitive information.
- Educate employees about how to avoid Phishing and phone pretexting scams.

### Pitch It

Properly dispose of what you no longer need.

- Create and implement information disposal practices.
- Dispose of paper records by shredding, burning, or pulverizing them.
- Defeat “dumpster divers” by encouraging your staff to separate the information that is safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace, including next to the photocopier.
- Use a “wipe” utility programs when disposing of old computers and portable storage devices.
- Give business travelers and employees who work from home a list of procedures for disposing of sensitive documents, old computers, and portable devices.

### Plan Ahead

Create a plan for responding to security incidents.

- Create a plan to respond to security incidents, and designate a response team led by a senior staff person(s).
- Draft contingency plans for how your business will respond to different kinds of security incidents. Some threats may come out of left field; others — a lost laptop or a hack attack, to name just two — are unfortunate, but foreseeable.
- Investigate security incidents immediately.
- Create a list of who to notify — inside or outside your organization — in the event of a security breach.
- Immediately disconnect a compromised computer from the Internet.

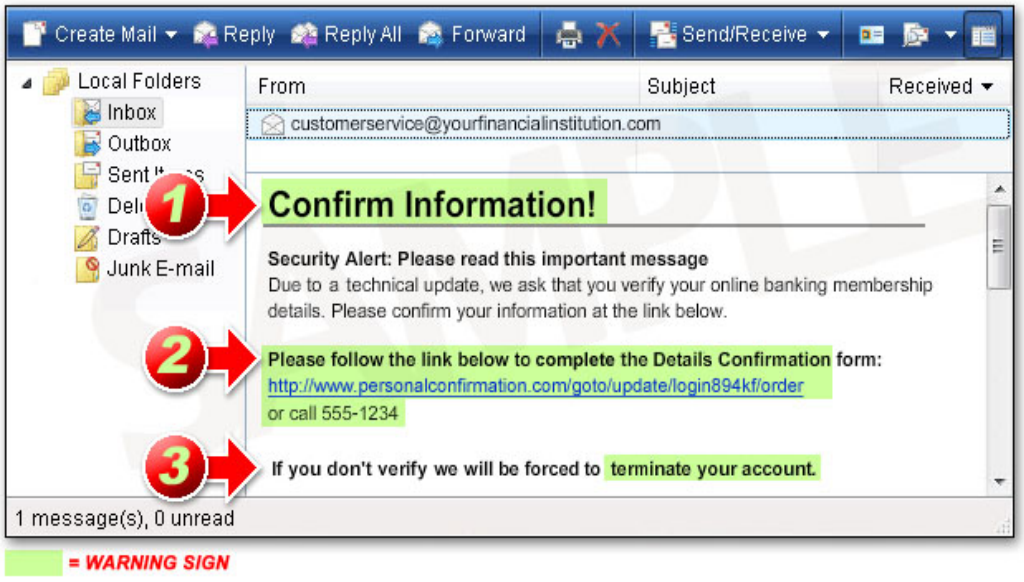
## E-mail Risk

Phishing is an e-mail scam used to steal your personal information. E-mail may appear in your inbox, claiming to be from your financial institution or another source. It may appear authentic but be careful - any e-mail requesting personal information or to "verify" account information is usually a scam. Do not respond to this type of e-mail and **do not** click on any link from this e-mail.

How to spot Phishing and other e-mail scams

- Any e-mail requesting personal information, or asking you to verify an account, is usually a scam, even if it looks authentic.
- The e-mail may ask you to change vendor payment information (i.e. wire instructions to a new correspondent bank).
- The e-mail may instruct you to click on a link, or call a phone number to update your account or even claim a prize, such as a sweepstake or lottery.
- The message will often threaten a dire consequence if you don't respond immediately, such as closing your account.

These are clear signs that someone is "Phishing" for your information.




Follow these steps to avoid e-mail scams

- Never respond to any e-mail asking for confidential information, even if it appears urgent. Chances are it is a fraudulent e-mail.
- Never click on a link from an unknown e-mail. Instead, type the known Website address for your bank or financial institution into your Internet browser.

- Do not call any phone number provided in a suspicious e-mail. It could be a fake phone number. Instead, call the phone number listed on the known Website address for your bank.
- Always use anti-virus and anti-spyware software on your computer, and keep them up-to-date.

Remember, e-mail is not a **secure** form of communication. So feel free to use your e-mail, but don't use it to send or receive confidential information. If you follow the four basic steps listed above, you can protect yourself from most phishing and other e-mail scams.

### Internet Risks

The Internet is a great place to browse and do business, however it can also be a dangerous place for identity theft if you don't know what to watch for or how to protect yourself. There are several types of malware – which means malicious software – that can infect your computer as you surf the web including:

- Viruses
- Spyware/Adware
- Trojan Horses
- Keystroke Loggers

These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal and/or business information. While "surfing" the Internet, follow these steps to protect your computer from the majority of Internet crime:

- Make sure you have anti-virus and anti-spyware software installed on your computer, keep them up-to-date, and run a full system scan at least weekly.
- Keep your computer operating system up to date, and your firewall turned on.
- 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. Opus Bank does not offer credit scores or credit reports. Run a full system anti-virus and anti-spyware scan to identify and safely remove spyware.
- Be careful when using public computers to perform any type of personal transactions. Just logging into a Website may give away passwords and other private information if spyware has been installed on that computer.

Following these steps will help protect you from the most common forms of identity theft while surfing the Internet.

### Telephone Risk

The telephone is one of the most often used sources for criminal activity. Here's how it works. Your phone rings. The caller claims to be from your financial institution, or any other source. They begin asking questions about you and your bank account information. Other telephone scams claim that you've won a sweepstake and ask for personal information in order to claim the "prize". These are attempts to obtain account information and/or steal your identity, and it happens to millions of Americans every year.

Protect yourself from telephone scams by following these steps to protect yourself from telephone scams:

- Never offer personal or business related information over the phone without verifying the caller's identity.
- If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.
- Do not call any phone number received in a voice message or e-mail asking for personal information. It could lead you to a phony answering system.

As a general guideline, be highly suspicious anytime you are requested to provide personal information over the phone.

### Opus Bank Contacts

You are protected in a variety of ways when you use Internet Banking; however it is important to contact Opus Bank in the event you that your company's online access has been compromised. Also, report any unauthorized or unexpected transactions immediately.

Your account is protected against fraudulent transactions in a number of ways, so monitor your account balances and transactions frequently. If you want to report suspicious activity in your account(s), or if you have questions about the security of your account(s), you can call us at: **(855) 678-7226** or e-mail us at mfraudunit@opusbank.com.

The security of your company's money and identity is as important to us as it is to you. Let's work together to protect it.

### Regulation E: Electronic Fund Transfers

This law is designed to protect 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.

# Business/Commercial Client Internet Banking Awareness and Education Program

The Electronic Fund Transfer Act (also known as Regulation E) was issued by the Board of Governors of the Federal Reserve System and adopted in 1978 as an add-on to the Consumer Credit Protection Act. The law and regulation establish the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services.

**Business/Commercial clients are not covered by Regulation E.** As a result, it is critical that business/commercial clients implement sound security practices within their places of business as outlined in this Program to reduce the risk of fraud and unauthorized transactions from occurring.

Good practices can keep business/commercial client's information secure.

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced onto your systems may go undetected for weeks or months. Account-draining transfers using stolen credentials may happen at any time and may go unnoticed depending on the frequency of your account monitoring efforts.

The good news is, if you follow sound business practices, you can protect your company:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.
- Manage the security of online banking with a single, dedicated computer used exclusively for online banking and cash management. This computer should not be connected to your business network, should not retrieve any e-mail messages, and should not be used for any online purpose except banking.
- Educate your employees about cybercrimes. Make sure your employees understand that just one infected computer can lead to an account takeover. Make them very conscious of the risk, and teach them to ask the question: "Does this e-mail or phone call make sense?" before they open attachments or provide information.
- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal e-mail. Such sites could inject malware into your network.
- Establish separate user accounts for every employee accessing financial information, and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal credentials. If your user permissions for online banking include administrative rights, don't use those credentials for day-to-day processing.
- Use approval tools in cash management to create dual control on payments. Requiring two people to issue a payment – one to set up the transaction and a second to approve the transaction – doubles the chances of stopping a criminal from draining your account.

Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

# Business/Commercial Client Internet Banking Awareness and Education Program

## Purpose

On June 28, 2011, the FFIEC (Federal Financial Institutions Examination Council) issued a supplement to the *Authentication in an Internet Banking Environment* guidance released in October 2005. The purpose of the supplement is to reinforce the guidance's risk-management framework and update the FFIEC member agencies* expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online banking environment.

The purpose of the Opus Bank Business/Commercial Client Internet Banking Awareness and Education Program (the "Program") is to ensure that our Internet Banking clients are aware of the risks of using Internet Banking. The Program will remind clients about the importance of security measures that can protect them from being victims of fraud. Specifically the program will address the importance of password security, using unique user accounts, and ensuring their computer systems used for Internet Banking have security software, such as firewalls, and updated anti-virus protection. The Program will include education about security threats, provide information to help them increase and maintain password security by enforcing a strong password requirement and periodic password changes. At Opus Bank, we strongly believe that public awareness of Internet banking risks and how to avoid them is the strongest weapon in the defense against monetary losses.

The following topics are intended to address the minimum elements that are part of Opus Bank's Business/Commercial Client Internet Banking and Customer Awareness and Education Program.

** The member agencies include the FRB, FDIC, NCUA, OCC and CFRB. For more information, please visit www.FFIEC.gov.*

**Additional Resources**

The following links are provided solely as a convenience to our Business/Commercial Online Banking clients. Opus Bank neither endorses nor guarantees in any way the organizations, services, or advice associated with these links. Opus Bank is not responsible for the accuracy of the content found on these sites.

- Identity Theft, Privacy, and Security Publications for Businesses
- OnGuard Online: Learn how to avoid Internet fraud, secure your computer, and protect your personal information.

Also

- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
- NIST's Risk Management Guide for Information Technology Systems (pdf)
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
- U.S. Computer Emergency Readiness Team (US-CERT)
- Carnegie Mellon Software Engineering Institute's CERT Coodination Center
- Center for Internet Security (CIS)
- The Open Web Application Security Project
- Institute for Security Technology Studies