



UNITED LABOR BANK f.s.b.

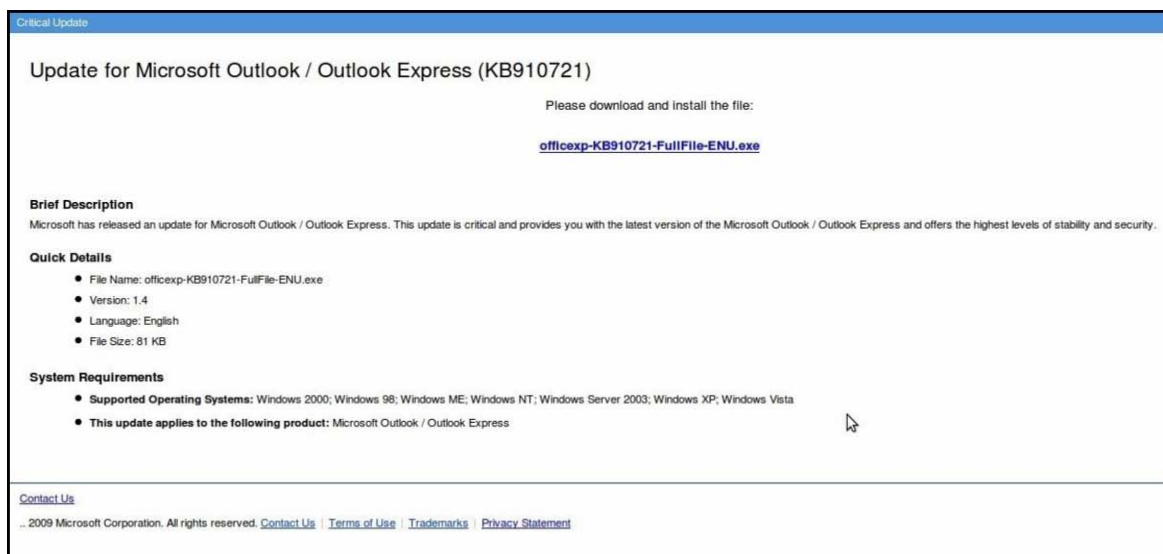
SECURITY RECOMMENDATIONS AND REQUIREMENTS FOR BUSINESS CUSTOMERS 4/1/2010

Background

There has been a shift in the online criminal world from primarily targeting of individuals to increased targeting of businesses. In the past 12 months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.

Compromise of the Customer

Typically compromise of the customer is carried out via a “spear phishing” e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. The e-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user’s computer which usually consists of a Trojan keystroke logger, which harvests the user’s corporate online banking credentials. Many types of spear-phishing have been used by criminal groups including messages impersonating the Better Business Bureau, US Court System, and UPS to name a few. The image below shows a recent example of a fraudulent Microsoft Update web site where receivers of “spear phishing” e-mails were taken after clicking the embedded link within the e-mail.



In this example the phishing e-mail was posing as a Microsoft Critical Update, thus bringing the user to a fictitious Microsoft page.

The Fraud

The customer's online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication system, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session.

The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unwitting individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.

Recommendations to Business and Corporate Customers

- Account Controls:
 - Reconciliation of all banking transactions on a **daily basis**.
 - Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Secure computer systems in your business including but not limited to:
 - If possible, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
 - Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack your computer.
 - Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
 - Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
 - Prohibit the use of "shared" usernames and passwords for online banking systems.
 - Use a different password for each website that is accessed.
 - Change the password a few times each year.
 - Never share username and password information for Online Services with third-party providers.
 - Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
 - Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
 - Ensure virus protection and security software are updated regularly.
 - Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
 - Consider installing spyware detection programs.
 - Avoid using an automatic login features that save usernames and passwords for online banking.
 - Never leave a computer unattended while using any online banking or investing service.
 - Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
- Immediately escalate any suspicious transactions to the financial institution particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.

Recommendations for Online Fraud Victims

In the event you are a victim of fraud, there are a number of immediate recommendations you should take to help protect your financial interests:

- Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connections to isolate the system from remote access.
- Immediately contact United Labor Bank so that the following actions may be taken as a priority to contain the incident:
 - Online access to the accounts be disabled.
 - Online Banking passwords changed.
 - New account(s) opened as appropriate.
 - Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
 - Additionally, ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.
- File a police report with the local police department and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.
- Maintain a written chronology of what happened, what was lost and the steps you took to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
- If you have conducted personal online banking from the business computer system, there are also potential identify theft aspects to the compromise. Verify your personal accounts and review the recommendation at the Federal Trade Commission's Identity Theft website.
- Have your network and systems reviewed by a qualified computer forensic/information security professional, if applicable.

Incident Reporting

We strongly encourage victims of cyber crime to contact their local FBI field office, <http://www.fbi.gov/contact/fo/fo.htm>, or file a complaint online at www.IC3.gov.