

Understanding e-mail scams, viruses, and spyware

MicroData Technical Brief

Abstract

June 12, 2005 – This brief is intended to give a user a basic understanding of some of the most common e-mail scams as well as common ways that e-mail is used to transmit viruses and spyware.

E-mail scams and phishing

- Typical format: E-mail purports to come from a financial institution or a vendor where you may have a credit card on file
- Strategy: The objective is to get you to follow a link to a website and enter your account and password information effectively giving the thieves access to your money or credit cards
- Who's affected? All computer users regardless of type of computer (Mac or PC) or operating system.
- Defense: Delete the e-mail. Some e-mail programs block all hyperlinks in messages as an additional defense

An e-mail is received in which users are lured into revealing potentially confidential personal information. This technique is called *phishing*. Users receive an e-mail message that typically claims to come from a bank, credit card company, or other financial institution. Usually the message will include a graphic of the company's logo and a message similar to the following (Citibank is referenced in this example):

On {any date may appear here} Citibank had to block some accounts in our system connected with money laundering, credit card fraud, terrorism and check fraud activity. The information in regards to those accounts has been passed to our correspondent banks, local, federal and international authorities.

Due to our extensive database operations some accounts may have been changed. We are asking our customers to check their checking and savings accounts if they are active or if their current balance is correct.

Citibank notifies all its customers in cases of high fraud or criminal activity and asks you to check your account's balances. If you suspect or have found any fraud activity on your account please let us know by logging in at the link below.

Clicking the supplied link takes you not to the bank's website, but to a criminal site usually in some foreign country (Korea and China are typical). Once on the site you'll find a realistic looking form asking you to enter your bank account information and password. Unknowingly supplying this info permits the thieves to steal monies or place orders for goods with your personal information.

While some antivirus vendors have included updates to block a specific location that is used by this attack, the criminals involved respond by simply closing down one web site and opening another.

To protect yourself from this type of threat, you should do the following:

- do not click on a hyperlink in any e-mail message that claims to come from a financial institution
- simply delete the e-mail

If you need to conduct on-line banking or perform other financial transactions, you should do the following:

- Always manually open a new web browser session and type in the home page address of your financial institution yourself.
- Once the home page is loaded, always verify that you have a secure connection to the web server you are connected to. In Internet Explorer, look for the small yellow padlock in the lower status bar of your browser window. If it's missing, you are probably not where you think you are as any reputable financial institution should have a secure site.
- If the yellow padlock is there indicating a secure connection, double click it to bring up the certificate for the website. The certificate allows you to verify that the website you are looking at is, in fact, the same as what you entered into the browser. If the URL referenced in the certificate is different than the URL of the page you are on, you should be suspicious of what the site is claiming and you should not enter financial or confidential information.
- Finally, if you ever have a question about on-line financial transactions, you should stop and call the institution involved and they will gladly assist you to ensure a secure and safe on-line session.

E-mail based Viruses and Spyware

The purpose of e-mail based viruses and spyware is two-fold: to infect the host system and to propagate to other systems. Infections can range from mildly annoying to destructive (corrupt computer and cause operation problems) to malicious (steal passwords and other data). Propagation to other systems can be

either by e-mail or simply by network connection. When e-mail is used, the virus usually has its own e-mail engine and the user may never know that mail is being sent on their behalf.

With proper antivirus, anti-spyware, and firewalls installed and configured on your computer and network, you are usually safe, but you still need to be vigilant in recognizing such threats and dealing with them appropriately. The following are two common types of threats.

Threat 1 – You receive a system e-mail from the postmaster about a failed message you never sent

- Typical format: The e-mail is a typical system e-mail from a mail system informing you that a mail message was not deliverable, but you never sent the message in question
- Strategy: This is the result of a virus from another computer system – not yours. You are simply seeing the byproduct of the virus operation.
- Who's affected? All computer users regardless of type of computer (Mac or PC) or operating system.
- Defense: These is nothing you need to do in this case

You may receive a large amount of email that either the sender has communicated they never sent you or the message seems to indicate you've sent a virus to someone; here's what is really going on:

Those messages you've received are from someone else's infected system sending to you, or where you appear to have been the sender, your e-mail address has been *spoofed*.

The way that many of these viruses/worms work is that when they infect a system, they create a mini-mail server that can be used to send copies of the virus to other users. The virus scans the infected system looking for any e-mail addresses it can find. These can be from address books or from anyone that the user has sent or received e-mail to or from. Then in order to mask where the virus-laden message came from and to encourage other users to open the e-mail, the virus randomly places e-mail addresses into the 'From' field - this is called *spoofing*. If the bogus reply address is yours, out-of-office replies, failure messages, and virus notifications will then be properly routed back to you. You haven't sent a virus or message to anyone, but the nature of how the virus/worm functions indicates to the receiver that it was you who sent it.

Threat 2 – E-Card Hoax

- Typical format: You receive an e-mail – often from an address you may recognize – informing you that you have received an electronic card
- Strategy: The e-mail message itself doesn't contain a virus or worm. The message contains a link to a website that will infect your machine if you click on it.
- Who's affected? PC users.
- Defense: Never follow an invitation for a link to an e-card. Simply delete the message.

This second threat only affects IBM compatible computer users. An e-mail message tries to entice a user to run an application that will infect the user's system (and network) with worms, spyware, or other malicious code. While this type of threat isn't new, the technique being employed tries to entice users to click on a hyperlink in the message by claiming that the user has received an 'e-card'. With the Thanksgiving and Christmas holidays approaching, this type of message has the potential to trick many users who are accustomed to sending and receiving e-cards.

The message has several possible subjects:

<Recipient> you have an E-Card from <Sender>
<Recipient> you have a greeting card from <Sender>.
<Recipient>, you have a funny card from <Sender>
<Recipient> you recently received a postcard sent by <Sender>
<Recipient> you just received a postcard from <Sender>
just emailed you a postcard -- <Sender>
just posted you a postcard - <Sender>
<Recipient> you have received a postcard sent by <Sender>
<Sender> today sent to you a postcard :<Recipient>

The e-mail message has content similar to the following - the referenced source will vary:

<Recipient>,
<Sender> has sent you a greeting card -- a postcard from Friend-Greetings.com. You can pickup your greeting card at Friend-Greetings.com by clicking on the link below.
<http://www.friend-greeting.com/203746/pickup.html?code=<blocked>&id=0811025>
Message:

<Recipient>
I just sent you a greeting card - please pick it up.
<Sender>

Clicking on the link takes the user to a site that will automatically install the damaging software. The infected system will then send out additional copies of the worm to other users that it finds in the mail application.

It's important to note that the sender's name may be spoofed (faked) so that you may recognize the individual. And because the message doesn't, in fact, contain a virus, worm, or any malicious code, antivirus software will not detect such threats.

To protect yourself against these threats, MicroData recommends that users simply delete any messages received that offer any type of e-card.

Threat 3 – Free applications, computer 'health' checkups, add-in toolbars, etc.

Typical format:	A website offers you a free application or service
Strategy:	You may get some sort of application, but you will also allow spyware to be installed on your computer
Who's affected?	Mostly PC users
Defense:	Do not install any free applications on your system unless you are 100% sure they come from a safe source. There is no automated defense for many of these threats as the user is intentionally choosing to install them on their computer

This type of spyware is particularly nasty as the spyware components are hidden under the guise of some sort of legitimate application, utility, add-in, or services. Many adult sites also install spyware.

Typical examples of such spyware include:

- Weather applications
- 'Smileys' or other add-ins for e-mail
- Toolbars for your web browser
- Computer health checkups that claim to 'tune up' or fix problems on your computer
- Adult sites

Defense against these applications is difficult because users are, in effect, infecting themselves by installing the applications or visiting the sites. Assuming you have current antivirus and anti-spyware software installed and properly configured, the best defense against such attacks is to never install any software on your computer unless you are 100% sure it is safe.