

---

# CONSUMER ALERT

MIKE COX  
ATTORNEY GENERAL

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern.

---

## FRAUDULENT E-MAIL THIEVES INTEND TO STEAL YOUR PERSONAL INFORMATION

### HOW THE SCAM WORKS

Crooks unleash fraudulent e-mail scams at a ferocious pace. The e-mail pretends to come from businesses the potential victims patronize – for example, Internet service providers, online payment services, well-known national retailers, and banks. Thieves make up some story (often basing part of the story in fact) designed to trick victims into providing personal information. The e-mail directs the recipient to click on a provided hyperlink to clear up the problem. The hyperlink leads to a server (usually in another country) on which a fraudulent imitation of a legitimate Web site appears. This scam is often referred to as "phishing" or "carding".

The deceived individual is then prompted to enter confidential personal information collected to perpetrate fraud or identity theft. The victim is usually then redirected to a legitimate Web site to obscure the fact that he or she just gave away personal financial information to crooks. You may recall hearing of these scams purporting to come from Best Buy, Citibank, eBay, Earth Link, FDIC (Federal Deposit Insurance Company), the IRS, PayPal, and U.S. Bank – just to name a few. A group that tracks this type of scam and posts information is located at [www.antiphishing.org](http://www.antiphishing.org).

In a new twist on "phishing" scams, identity thieves send consumers fraudulent e-mails from popular on-line merchants. The e-mail looks like an order confirmation e-mail, commonly sent by merchants to consumers that recently made an on-line purchase. To make the e-mail even more deceptive, the scammers put an order number in the subject

---

Michigan Attorney General Consumer Alerts are available at [www.michigan.gov/ag](http://www.michigan.gov/ag)  
Toll free 1-877-765-8388

---

line of the e-mail, luring consumers into opening the e-mail. The problem is opening an e-mail like this, even if you do not open the attachment, can unleash a dangerous virus or spyware onto your computer.

## **DO NOT PROVIDE PERSONAL INFORMATION TO SOMEONE WHO CALLS OR E-MAILS YOU**

Regardless of who they claim to be, treat people who call or e-mail you seeking personal or financial information as potential thieves who may be trying to steal your identity. Resist their alarming or believable scenarios and urge to update, validate, or confirm sensitive information. Do **NOT** provide people who call or e-mail you with any personal information. Remember the thieves constantly change their disguised identity by adopting a new alias.

## **PROTECT YOURSELF**

Follow the Federal Trade Commission's suggested guidance:

- **If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.** Legitimate companies don't ask for this information via e-mail.
- **If you receive an e-mail from an on-line merchant, make sure you compare the order number in the subject line of the e-mail to the receipt you printed from the merchant's Web site when you completed your order.** If the order number in the subject line does not match the order number on your receipt, **do not open the e-mail!** Delete it immediately.
- If you are concerned about your account, contact the organization mentioned in the e-mail using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser – phishers can make links look like they go to one place, but that actually send you to a different site.
- **Use anti-virus software and a firewall, and keep them up to date.** Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones, that can effectively reverse the damage, and that updates

automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Don't e-mail personal or financial information.** E-mail is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a Web site that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- **Be cautious about opening any attachment or downloading any files from e-mails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **Forward spam that is phishing for information** to [spam@uce.gov](mailto:spam@uce.gov) and to the company, bank, or organization impersonated in the phishing e-mail. Most organizations have information on their Web sites about where to report problems.

**If you believe you've been scammed, file your complaint at [ftc.gov](http://ftc.gov)**, and then visit the FTC's **Identity Theft Web site** at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See [www.annualcreditreport.com](http://www.annualcreditreport.com) for details on ordering a free annual credit report.

For Michigan specific information on Identity Theft, see Attorney General's Consumer Alert entitled, "Identity Theft Information for Michigan Consumers" (available at <http://www.michigan.gov/ag/0,1607,7-164--80479--,00.html>). If you fall victim to one of these scams, scrupulously monitor your accounts and be prepared to file a police report if you detect any fraudulent activity.

## **FILE A COMPLAINT**

If you encounter a company that insists you are responsible for an identity theft related debt, please contact the Attorney General's Consumer Protection Division at:

Consumer Protection Division  
P.O. Box 30213  
Lansing, MI 48909  
517-373-1140  
Fax: 517-241-3771  
Toll free 877-765-8388  
[www.michigan.gov/ag](http://www.michigan.gov/ag) (online complaint form available)