Malware Attack in Progress; Please Read

Some of our clients have reported receiving a fraudulent email that reads similar to what is shown below:

```
-----Original Message-----
From: Fiserv Secure Notification [mailto:secure.notification@fiserv.com]
Sent: Monday, June 24, 2013 9:28 AM
To:
Subject: Fiserv Secure Email Notification - [random alphanumeric characters]

You have received a secure message

Read your secure message by opening the attachment, SecureMessage_[random
alphanumeric characters] .zip.

The attached file contains the encrypted message that you have received.

To decrypt the message use the following password - Iu1JsoKaQ

To read the encrypted message, complete the following steps:

- Double-click the encrypted message file attachment to download the file to
your computer.
- Select whether to open the file or save it to your hard drive. Opening the
file displays the attachment in a new browser window.
- The message is password-protected, enter your password to open it.

To access from a mobile device, forward this message to mobile
@res.fiserv.com to receive a mobile login URL.

If you have concerns about the validity of this message, please contact the
sender directly. For questions about secure e-mail encryption service, please
contact technical support at 888.493.7980.

2000-2013 Fiserv Secure Systems, Inc. All rights reserved.
--------------------------------------------------------------------------
```

If you receive this email, do not attempt to download nor open the attachment and do not reply to it. Delete it from all of your devices.

The email falsely represents itself as coming from our organization, but it is not associated with our organization in any way. Our systems were not utilized to conduct this fraudulent email scheme and our systems remain secure. The email contains an attachment. Clicking on the attachment could disrupt or damage systems.

The risk associated with malware can be lowered as follows:

1. If the request comes in the form of an email, do not open it, do not open its attachments, and do not reply to it.

2. If consumers receive such requests, they should never comply with them, as we never send information in this manner.
3. In addition, our organization offers "Online Business Banking Security Awareness," a complementary training course for our clients and their business customers. For more information on the training, or to request the training, contact CustomerSecurityAwareness@fiserv.com
4. Install and use anti-virus software, and update it as recommended by its supplier.
5. Limit Internet access for business computers to websites approved for business use and block all other websites.
6. Employ multiple and layered data security tools. Data thieves often know a great deal about one or more data security tools. Experience finds that layering multiple security tools and customizing them to meet the needs of specific industries and companies reduces the likelihood that data thieves will succeed.

As background information, malware is defined as software that is intended to damage, disable, steal data, or disable computers and computer systems. These documents falsely represent themselves as being from legitimate organizations.

Often the email contains an attachment, or directs the recipient to a malicious website. Some recipients, believing that the email is from a legitimate organization, may comply with the requests, which may infect the computer or the computer network.

For additional information, you may want to visit:

1. *Internet Crime Complaint Center* (http://www.ic3.gov/default.aspx) a partnership of the Federal Bureau of Investigation and the National White Collar Crime Center.
2. *Anti-Phishing Working Group* (http://www.antiphishing.org/), a coalition of industry, law enforcement and government entities focused on unifying the response to cybercrime.

If you wish to discuss this or have questions, please contact your account representative.