Valentine's Day: What's Fraud Got To Do With It? Everything!

By Denise Richardson

They show up in your text or e-mail inbox, messages with a subject line that reads, "You have received a Valentine's card" or "Your sweetheart has sent you a Valentine's Day greeting." Some may even indicate that, "The flowers you ordered for your sweetie won't be delivered unless you log in and re-enter your credit card information." But look out, Cupid. With February 14th fast approaching, you need to be on the alert for text and spam e-mails that are anything but romantic!

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Tens of millions of fake Valentine's Day greeting-card messages will be sent out this Valentine's Day, and it's likely you will receive one. The e-mail may direct you to click on a link to retrieve your special electronic e-card. Beware. When you click on the link, a virus and malicious malware may be triggered to download onto your computer. The spyware that is installed often includes a key-logger program, which tracks the sites you visit while also logging every keystroke you make on your computer. Key-logger software can record user names, passwords, account numbers and personal PIN numbers, too. Ultimately, every key you press on the keyboard is captured. Everything you type into word-processing documents, spreadsheets or e-mail programs is recorded too.

These spyware and malware programs typically run without your knowledge and are difficult to detect, and they continue to run in the background until they are detected and removed. If you receive a notice that a greeting card has been sent to you, before you even consider opening on an attachment or clicking on an embedded link, first check with the person it claims to be from and determine whether or not they actually sent it. Under no circumstances should you blindly trust that the card is legitimate simply because the e-mail looks legitimate. If you discover that the e-mail is spam, delete it

immediately--without clicking on the links.

If you have already received a greeting card message and clicked on its links, there are still steps you can take to protect yourself. First, you should install up-to-date virus protection on your computer and run a full virus scan on your hard drive. If you find that your computer has been infected, you should then place a fraud alert on your credit files with each of the big three credit reporting agencies (Trans Union, Experian and Equifax). You only need to contact one credit bureau and they will alert the other two agencies. Sorry to say, if you want the alert to stay on your accounts, you will need to reset it every three months days. After 90 days, the alert automatically expires.

With fraud alerts in place, creditors, lenders, or other prospective users of your consumer report should take steps to verify your identity before they can issue new credit, increase credit lines, and obtain utilities, cell phones or new loans. I know that many people believe when someone else is trying to use your identity to get credit, any potential creditor would take steps to verify the identity of the applicant---with or without a fraud alert in place; unfortunately, they don't. If you don't plan on purchasing anything that would require a creditor to check your credit; consider paying for a credit freeze. Though fraud alerts are free, a credit freeze will require you to pay each credit bureau. (Find additional info here: Extended Fraud Alerts and Credit Freezes)

It's also important to note that often scammers will instruct you to call a provided phone number. Never dial an unsolicited number provided in an unsolicited e-mail, text or voice mail, even if it purports to come from a company you deal with regularly. Instead, take the time to look up the legitimate phone number of the company and call that instead.

There are, of course, variations to these types of phishing and spoofing scams. Spoofing scams occur when criminals create a false or "shadow" copy of a real website or e-mail. This allows the "spoofer" to acquire personal information such as passwords, credit card numbers, and account numbers. Even though the e-mail looks like the real thing--complete with authentic logos and working web links--it's just an elaborate fake. The website where you're instructed to enter your account information into -is also fake. In some instances, really slick spoofers direct you to a genuine website and then arrange a pop up a window to appear over the site. Any information entered, goes straight to the spoofer. Your information will most likely be sold to criminals who'll use it to drain your accounts, ruin your credit and steal you and your sweetheart's name!

Follow these tips to prevent having more than your heart stolen this Valentine's Day!

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files as these files may contain viruses.
- Open cards or attachments only after verifying the known sender ---did actually send it.
- Avoid filling out forms in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link that you are actually directed to.
- Log on to the official website instead of "linking" to it from an unsolicited e-mail.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
- Make sure you have a firewall and up-to-date antivirus software running on your computer at all times.
- Update any available Security Patches.

You might want to think twice before sending an electronic Valentine's Day Card this year. Don't take your identity --or sweetheart's security--for granted. Sharing your Valentine's Day message personally will help you, and your valentine, avoid falling victim to online threats.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow ACCESS