Criminal Justice Connections
An employee publication of the Texas Department of Criminal Justice
September 2017

Policies and Benefits

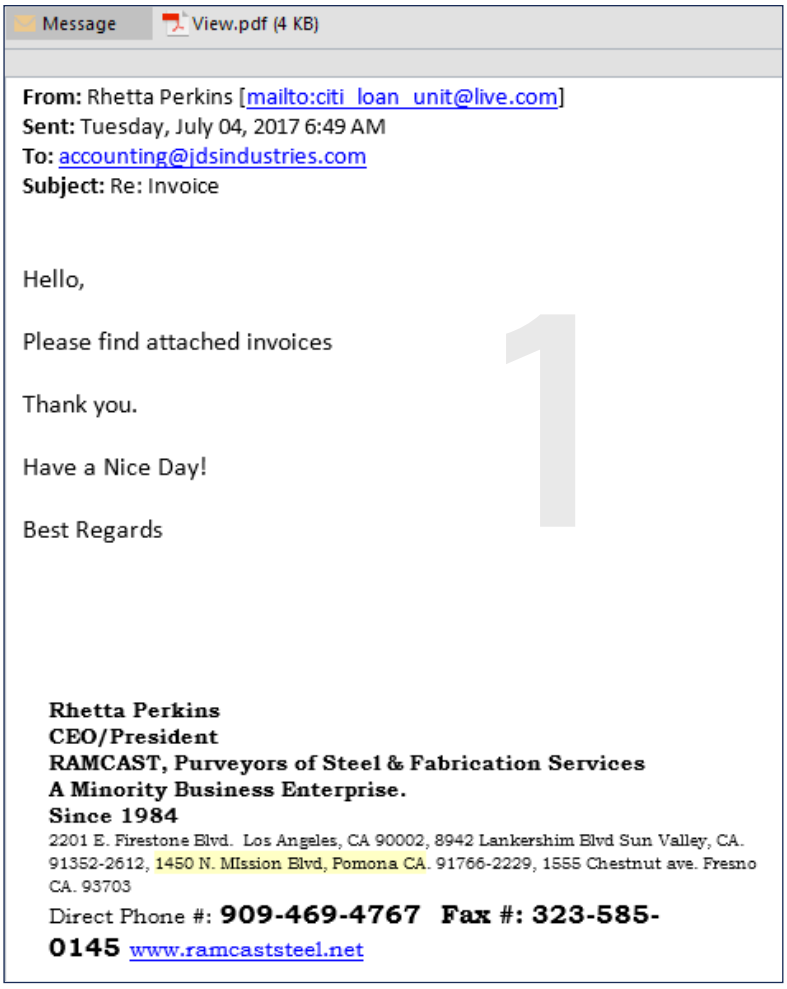
Information Security: how to recognize, report malicious email

Malicious emails continue to be the most popular method for launching a phishing or malware attack against computer users. According to the 2017 Internet Security Threat Report from Symantec Corporation, a company specializing in software security, one in every 131 emails sent in 2016 contained malware. Here are a few tips on how to avoid trouble by recognizing and reporting malicious email.

Take a good look at the email in Figure 1 and make a list of things that seem odd.

The attachment with this email contained a link to a phishing website, but it could have just as easily contained malware. The goal of the malicious actor who sent this email is to get you to open the PDF file. All the following are attempts to make the source – and the attachment - seem legitimate:

- The word "accounting" in an email address near the top of the message.
- The "Re:" prefix in the subject suggesting that you or someone in your organization requested the invoice in a past email.
- The natural sounding message body.
- The signature block of a seemingly respectable business person based in America.


Message View.pdf (4 KB)

From: Rhetta Perkins [mailto:citi_loan_unit@live.com]
Sent: Tuesday, July 04, 2017 6:49 AM
To: accounting@jdsindustries.com
Subject: Re: Invoice

Hello,

Please find attached invoices

Thank you.

Have a Nice Day!

Best Regards

1

Rhetta Perkins
CEO/President
RAMCAST, Purveyors of Steel & Fabrication Services
A Minority Business Enterprise.
Since 1984
2201 E. Firestone Blvd. Los Angeles, CA 90002, 8942 Lankershim Blvd Sun Valley, CA. 91352-2612, 1450 N. MIssion Blvd, Pomona CA. 91766-2229, 1555 Chestnut ave. Fresno CA. 93703
Direct Phone #: **909-469-4767** **Fax #: 323-585-0145** www.ramcaststeel.net

CONTINUED ON PAGE 2

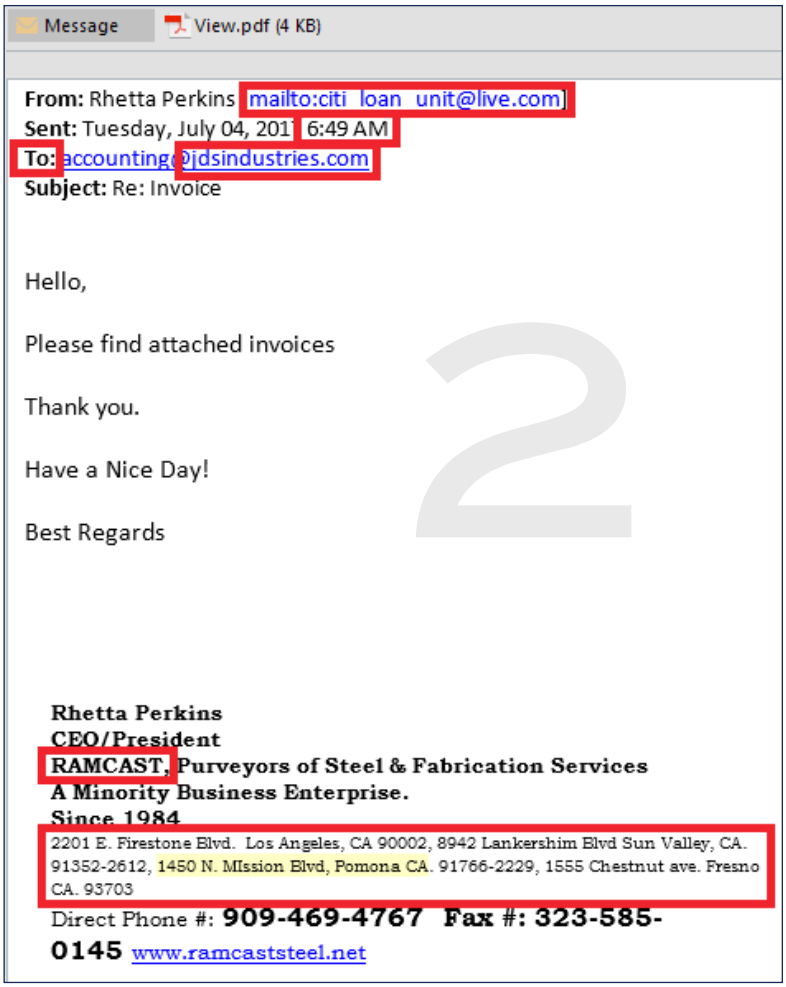
CONTINUED FROM PAGE 1

Now, compare your list of red flags to the items circled in red in Figure 2.

The first and most telling clue is the address that the email originated from and how it looks completely unrelated to the business in the signature block.

Another red flag is a common tactic found in malicious emails: the receiving address (your address) is not listed in the "To:" field. Instead, that field shows a legitimate-looking accounting address (accounting@jdindustries.com) to trick you into thinking the email may have come from that address, rather than the one in the "From:" field.

Some malicious emails can be spotted by taking note of the geographic locations listed in signature blocks and indicated by telephone numbers. This email example claims to have originated from California, and you'll notice that all of their offices are exclusively in California, which makes it unlikely they would do business with a Texas state agency. Also, the email was received at 6:49 a.m. Central Time, which means it would have been sent at 4:49 a.m. Pacific Time, another good reason to doubt its legitimacy.


Message View.pdf (4 KB)

From: Rhetta Perkins [mailto:citi_loan_unit@live.com]
Sent: Tuesday, July 04, 201 6:49 AM
To: accounting@jdsindustries.com
Subject: Re: Invoice

Hello,

Please find attached invoices

Thank you.

Have a Nice Day!

Best Regards

2

Rhetta Perkins
CEO/President
RAMCAST, Purveyors of Steel & Fabrication Services
A Minority Business Enterprise.
Since 1984
2201 E. Firestone Blvd. Los Angeles, CA 90002, 8942 Lankershim Blvd Sun Valley, CA. 91352-2612, 1450 N. MIssion Blvd, Pomona CA. 91766-2229, 1555 Chestnut ave. Fresno CA. 93703
Direct Phone #: **909-469-4767 Fax #: 323-585-0145** www.ramcaststeel.net

Here are some other ways to protect yourself from malicious emails:

- Scrutinize every detail of an email before opening the attachment or responding to the sender. NEVER open an attachment if you have any doubts about its authenticity.
- Alert TDCJ's Office of the Information Security Officer (contact information below) if you find any of the red flags listed above, or if you have other reasons to believe an email may not be safe.
- Never enter any of your TDCJ login details into websites or forms that are not hosted by TDCJ, which is indicated by a URL ending with tdcj.texas.gov. Never give your login details to anyone.
- Notify the OISO immediately if you think your login details have been compromised or your PC is infected.

If you have any questions about spotting malicious emails or any other aspect of information security, contact the agency's Office of the Information Security Officer at 936-437-1800 or ISO@tdcj.texas.gov. ▲