

From: Salesforce.com Security [mailto:email@salesforce.rsys1.com]
Sent: Tuesday, October 30, 2007 8:22 AM
To:
Subject: Urgent 10/29 Security Alert: Do Not Open "FTC" Email



Salesforce Admins,

Please read this urgent security warning and notify your organization's security department as soon as possible.

Today, many of our customers received a malicious email that appears to have been circulated on the internet. This message was a bogus email from the "FTC Fraud Department", and had malware attached which installs itself to a user's PC and logs keystrokes in an attempt to gain password or account access. This email should not be opened, and any users that have inadvertently opened it should cease use of their machines until your security department can evaluate them.

Here is a link to the FTC site with further information and updates:
<http://www.ftc.gov/opa/2007/10/bogus.shtm>

Report any suspicious emails to security@salesforce.com.

For your reference, a copy of the text from their site has also been pasted below. For security best practices, you can always view our security updates at <http://trust.salesforce.com/security.html>, or contact us directly at security@salesforce.com.

Phishing and malware are on the rise, but every customer can take a few critical steps to help fend off threats. Salesforce.com offers many technologies for improving your security. After you address the "FTC" email issue, salesforce.com strongly recommends your security team contact us for a security review. To schedule this review, please send an email to security@salesforce.com.

Thanks,

Security Team at Salesforce.com

Don't Open Bogus Email that Claims to Come From the FTC

Email That States It's From the FTC's 'Fraud Department' Has Virus Attached

A bogus email is circulating that says it is from the Federal Trade Commission, referencing a 'complaint' filed with the FTC against the email's recipient. The email includes links and an attachment that download a virus. As with any suspicious email, the FTC warns recipients not to click on links within the email and not to open any attachments.

The spoof email includes a phony sender's address, making it appear the email is from 'frauddep@ftc.gov' and also spoofs the return-path and reply-to fields to hide the email's true origin. While the email includes the FTC seal, it has grammatical errors, misspellings, and incorrect syntax. Recipients should forward the email to spam@uce.gov and then delete it. Emails sent to that address are kept in the FTC's spam database to assist with investigations.

Simply opening the email does not appear to cause harm. However, it is likely that anyone who has opened the email's attachment or clicked on the links has downloaded the virus on their computer, and should run an anti-virus program. The virus appears to install a 'key logger' that could potentially grab passwords and account numbers. More information about bogus emails, phishing, and virus protection is available at www.OnGuardOnline.gov.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to more than 1,600 civil and criminal law enforcement agencies in the U.S. and abroad. For free information on a variety of consumer topics, click <http://ftc.gov/bcp/consumer.shtm>.

35,300 Customers 700+ Applications 15 Languages

© Copyright 2007 salesforce.com, inc. • All rights reserved • Various trademarks held by their respective owners
salesforce.com | One Market Street, Suite 300 | San Francisco, CA 94105

This message was sent by salesforce.com.
[Click here](#) if you prefer not to receive future e-mail from salesforce.com.
[Click here](#) to view our permission marketing policy.