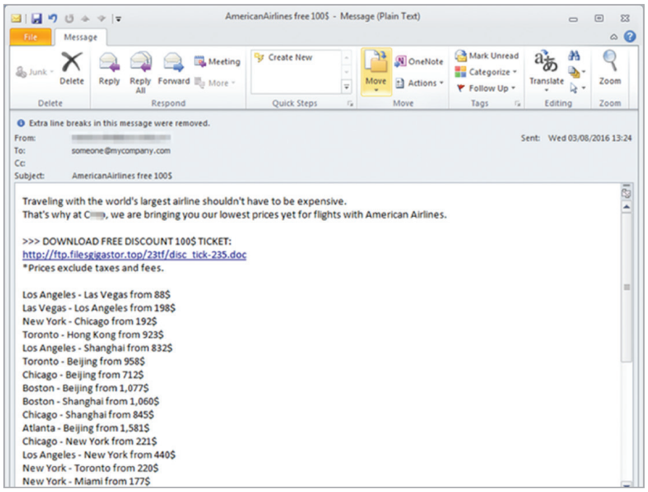
Avoiding Ransomware Attacks

CYBER SECURITY SEPTEMBER 2017

Ransomware is a type of malware designed to encrypt users' files or lock their operating systems so attackers can demand a ransom payment. According to a 2016 Symantec report, the average ransom demand is almost $700 and "consumers are the most likely victims of ransomware, accounting for 57 percent of all infections between January 2015 and April 2016."

Similar to a phishing attack, ransomware executes when a user is lured to click on an infected link or e-mail attachment or to download a file or software drive while visiting a rogue website. Sophisticated social engineering techniques are used to entice users to take the desired action; examples include:

- An embedded malicious link in an e-mail offers a cheap airfare ticket ***(see Figure 1)***;
- An e-mail that appears to be from Google Chrome or Facebook invites recipients to click on an image to update their web browser ***(see figure 2)***; or
- A well-crafted website mimics a legitimate website and prompts users to download a file or install an update that locks their PC or laptop.



Extra line breaks in this message were removed.

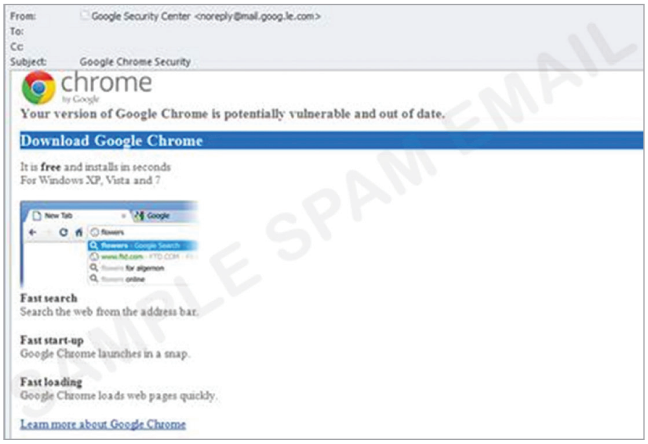
From: [redacted]
Sent: Wed 03/08/2016 13:24
To: someone@mycompany.com
Cc:
Subject: AmericanAirlines free 100$

Traveling with the world's largest airline shouldn't have to be expensive.
That's why at C[redacted], we are bringing you our lowest prices yet for flights with American Airlines.

>>> DOWNLOAD FREE DISCOUNT 100$ TICKET:
http://ftp.filesgigastor.top/23tf/disc_tick-235.doc
*Prices exclude taxes and fees.

Los Angeles - Las Vegas from 88$
Las Vegas - Los Angeles from 198$
New York - Chicago from 192$
Toronto - Hong Kong from 923$
Los Angeles - Shanghai from 832$
Toronto - Beijing from 958$
Chicago - Beijing from 712$
Boston - Beijing from 1,077$
Boston - Shanghai from 1,060$
Chicago - Shanghai from 845$
Atlanta - Beijing from 1,581$
Chicago - New York from 221$
Los Angeles - New York from 440$
New York - Toronto from 220$
New York - Miami from 177$

Figure 1. *Phishing e-mail with ransomware embedded in a link*



From: Google Security Center <noreply@mail.goog.le.com>
To:
Cc:
Subject: Google Chrome Security

Your version of Google Chrome is potentially vulnerable and out of date.

Download Google Chrome

It is **free** and installs in seconds
For Windows XP, Vista and 7

Fast search
Search the web from the address bar.

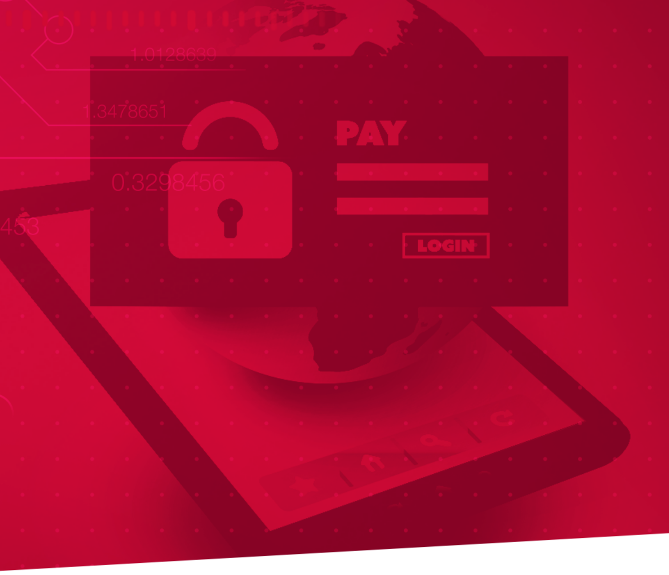
Fast start-up
Google Chrome launches in a snap.

Fast loading
Google Chrome loads web pages quickly.

Learn more about Google Chrome

Figure 2. *A fake Google Chrome e-mail*

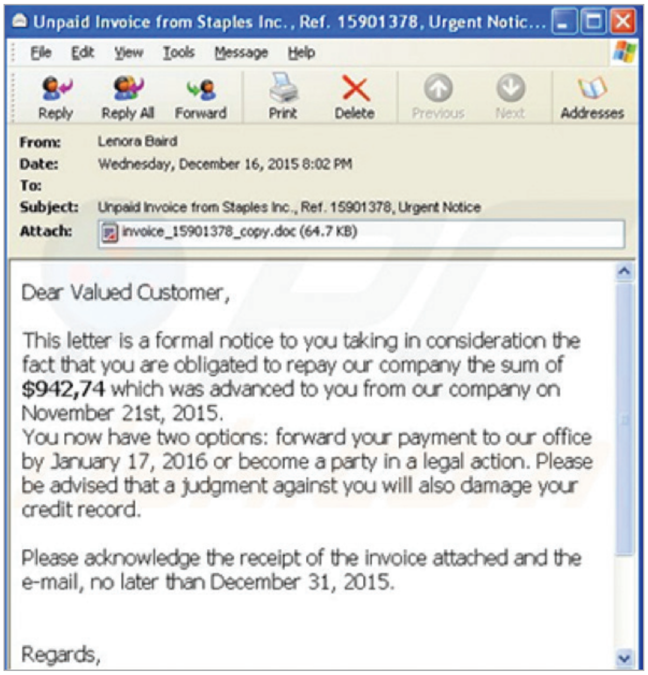
Avoiding Ransomware Attacks



CYBER SECURITY SEPTEMBER 2017

To avoid becoming a victim of ransomware, users can follow these tips:

- Delete any suspicious e-mail. Messages from unverified sources or from known sources that offer deals that sound too good to be true are most likely malicious ***(see figure 3)***. If in doubt, contact the alleged source by phone or by using a known, public e-mail address to verify the message's authenticity.
- Install and maintain up-to-date antivirus software. Keeping your operating system updated with the latest virus definitions will ensure that your security software can detect the latest malware variations.
- Update all devices, software, and plug-ins on a regular basis. Check for operating system, software, and plug-in updates often — or, if possible, set up automatic updates — to minimize the likelihood of someone holding your computer or files for ransom.
- Back up your files. Back up the files on your computer, laptop, or mobile devices frequently so you don't have to pay the ransom to access locked files.
- Avoid clicking on unverified e-mail links or attachments. Suspicious links might carry ransomware (such as the CryptoLocker Trojan).
- Use e-mail filtering options whenever possible. E-mail or spam filtering can stop a malicious message from reaching your inbox.



From: Lenora Baird
Date: Wednesday, December 16, 2015 8:02 PM
To:
Subject: Unpaid Invoice from Staples Inc., Ref. 15901378, Urgent Notice
Attach: invoice_15901378_copy.doc (64.7 KB)

Dear Valued Customer,

This letter is a formal notice to you taking in consideration the fact that you are obligated to repay our company the sum of **$942,74** which was advanced to you from our company on November 21st, 2015.
You now have two options: forward your payment to our office by January 17, 2016 or become a party in a legal action. Please be advised that a judgment against you will also damage your credit record.

Please acknowledge the receipt of the invoice attached and the e-mail, no later than December 31, 2015.

Regards,

Figure 3. *An example ransomware e-mail message*