Phishing and Ransomware



Think before you click!

FROM

- Does the sender look unfamiliar to you?
- If you know the sender, is the content different from what they would send?
- When you hover the address, is it different from what is in the header?

SUBJECT

- Does it imply you must take action?
- Does the language seem out of place?
- Does the subject line make you feel like you did something wrong?

TO

- Is there nothing in the To: field?
- Are there people in the To: field you don't know?
- Is your name spelled wrong?

DATE

• Was the email sent at a time that does not make sense?

ATTACHMENTS

- Is there an attachment? Don't open it!
- Does the attachment end in anything other than .txt?
- Did it ask you to enable macros (If you did open it)?

HYPERLINKS

- Is there a hyperlink in the email?
- When you hover the link does it show a different site than where it claims to go?

OTHER INFORMATION

- Is the email from a company that you typically don't get emails from?
- Does the grammar in the email seem wrong? In this example the user says "to be sure document is been viewed", obviously something Dropbox would not say, even if they did email you.

hvoice 1343.docx

Michael Drackley <mdrackley@groupon.com>

Michael used Dropbox to share some files with you. We need to verify your all address to be so document

is been viewed by You! http://zfmin.org/dl/gdoc/index.php Click to follow link

NOTE: You are accessing a highly secured important

Document.

Thanks!

Important Document

- The Dropbox Team

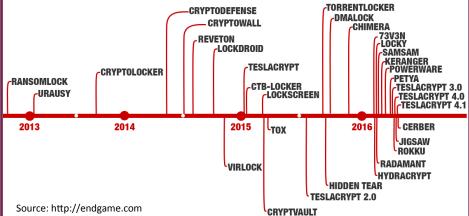
Hover the link, is it going where it says it is?

Mike Drackley

Merchant Development Manager-Things To Do

Desk: 773 696 4124 Emili mdracklev@groupon.com

Ransomware threats increasing and getting much smarter. TORRENTLOCKER CRYPTODEFENSE -DMALOCK -CHIMERA CRYPTOWALL



PRECAUTIONS

- Follow the same behaviour above for downloads and clicking hyperlinks when you are browsing.
- Have a good backup, preferably on a separate media or off-site cloud based. Image backups are even more protected from attacks.
- Install and maintain updates on a good antivirus/malware program.
- Install a good second generation firewall with malware protection.

