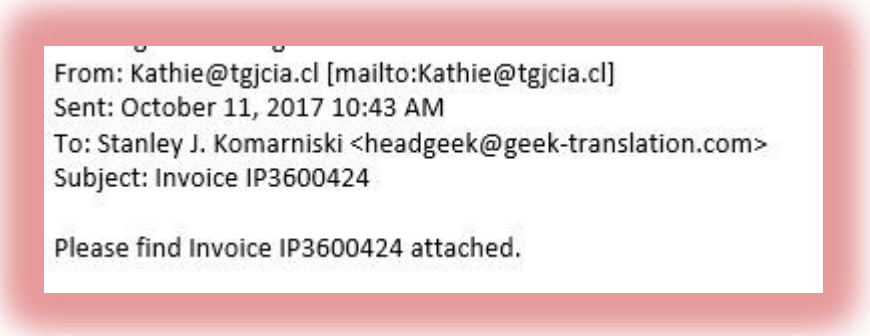
SPAM DOCUMENT…

Purpose: It is my hope with this document that it will help you recognize spam emails and know how to avoid the traps that are set in them. Remember a spam email is only annoying, until you click a link or open the attachment. When you do click or open anything with this spam email, it can have catastrophic results.

Following are examples of emails that I have received…

The Invoice:


From: Kathie@tgjcia.cl [mailto:Kathie@tgjcia.cl]
Sent: October 11, 2017 10:43 AM
To: Stanley J. Komarniski <headgeek@geek-translation.com>
Subject: Invoice IP3600424

Please find Invoice IP3600424 attached.

This is a common email. Sometimes it includes an attachment with a file that will infect your pc, or a link that will direct you to a fake website for payment. It might sometimes even include a familiar email address of someone you know.

The Website Notice:


From: noreply@paiddomain.biz [mailto:noreply@paiddomain.biz]
Sent: October 11, 2017 10:47 AM
To: Stanley J. Komarniski <headgeek@geek-translation.com>
Subject: Fwd: Attn: geek-translation.com Notice of Registration Soon

Fwd: Attn: geek-translation.com Notice of Registration Soon

Domain Name: geek-translation.com

Bill To:

Invoice # OCT-3-1199-4847600

Again, since I host my own websites, I know immediately this is fake. However, its official looking status has fooled many into paying for or allowing others control of their websites.

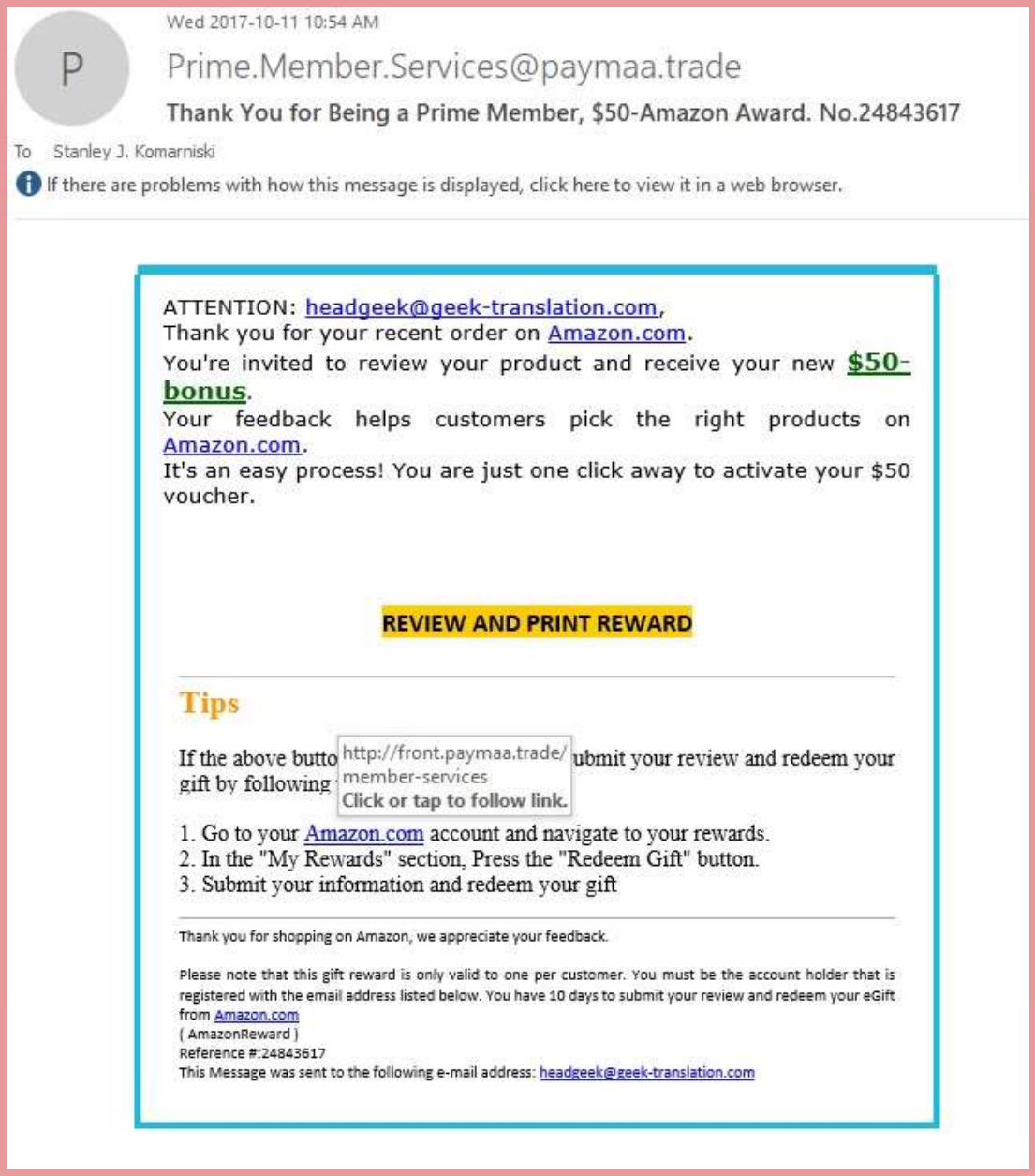
The Long lost relative:

From: thomas.kistler@foxmail.com [mailto:thomas.kistler@foxmail.com]
Sent: October 11, 2017 10:49 AM
To: Recipients <thomas.kistler@foxmail.com>
Subject: BUSINESS OFFER

Hello,
I am sorry if I disturb you but I have a very great business opportunity to discuss with you, kindly get back to me on my personal email address and I will explain details of the deal to you.
thomas.kistler@swissmail.com.
I am Thomas Kistler, (Chief executive officer) of AKB Privatbank Zürich AG, Zurich, Switzerland.
Await your response.
Mr.Thomas Kistler
(Chief executive officer)
(Foreign Remittance/Allocation Dept.)
AKB Privatbank Zürich AG.
Website: www.akbprivatbank.ch
https://de.wikipedia.org/wiki/AKB_Privatbank_Zürich

I have even received these from those trying to fake messages from relatives. Sometimes they contain messages of an inheritance, but the premise is still the same. Get me to click links to either infect my computer or get my money.

Online site Purchasing:



Wed 2017-10-11 10:54 AM

P

Prime.Member.Services@paymaa.trade

Thank You for Being a Prime Member, $50-Amazon Award. No.24843617

To Stanley J. Komarniski

If there are problems with how this message is displayed, click here to view it in a web browser.

ATTENTION: headgeek@geek-translation.com,
Thank you for your recent order on Amazon.com.
You're invited to review your product and receive your new **$50-bonus**.
Your feedback helps customers pick the right products on Amazon.com.
It's an easy process! You are just one click away to activate your $50 voucher.

REVIEW AND PRINT REWARD

Tips

If the above butto http://front.paymaa.trade/member-services Click or tap to follow link. ubmit your review and redeem your gift by following

1. Go to your Amazon.com account and navigate to your rewards.
2. In the "My Rewards" section, Press the "Redeem Gift" button.
3. Submit your information and redeem your gift

Thank you for shopping on Amazon, we appreciate your feedback.

Please note that this gift reward is only valid to one per customer. You must be the account holder that is registered with the email address listed below. You have 10 days to submit your review and redeem your eGift from Amazon.com
(AmazonReward)
Reference #:24843617
This Message was sent to the following e-mail address: headgeek@geek-translation.com

This one is one of the most effective as it looks official. How would they know you use amazon to purchase? They don't but the odds are high when they send millions of emails that someone would be an amazon customer. Notice the link in the center by number one. It shows amazon.com, however if you clicked that link the box above shows you that it would not take you to the amazon website. It would take you to a site that is tricking you into revealing your amazon account so they can purchase items using your account.

Currently as of 11am this morning, I have received **375 spam emails** with different variations of the ones above. However, with the filtering in my email server, for the most part most of these emails are filtered out. If they were not filtered, any legitimate emails would be lost in all the noise. Most email servers deploy some type of spam detection system. These systems must be maintained and upgraded as the spammers change their methods for sending this spam. This is an ongoing issue that will continue until everyone uses a secure email system.

Protecting yourself from spam:

1. Make sure that the person sending the email is legit. It can be easily done by looking at the from address…
   eg. FROM: joeblow@matrixgroup.ca [spammer@nowhere.com]
   - even though it shows a valid email at the beginning, the actual email is contained in the square brackets.
2. Never ever, reply to, forward these emails
   - if you do, your account will be flagged for sending spam. Since you sent the spam email…
   - if you need to confirm the email, send the email as an attachment to the actual email address to confirm
3. Never ever, click any links contained in the emails
   - if you click a link you confirm to the spammer that there is someone at the end of this email address
   - you could infect your pc with any files that are downloaded to your pc
4. When you get these emails and they are spam, right click on them and mark them as spam. Or better yet, delete them immediately!
5. If you believe you have opened an infected attachment, turn off your computer immediately and contact tech support. This will prevent a network wide infection and prevent the virus from damaging your files.

What can be done to eliminate spam?:

Nothing! Microsoft has been working on a way to eliminate spam for 20 years with no success. However we can minimize the amount of spam we receive by being careful with the emails we receive.

Why do the spammers Spam?:

- Money - plain and simple
- They sell our email addresses in the dark web for about a penny each for unconfirmed
- When we click a link in these fake emails, the email addresses become confirmed and are worth 5 cents each. It does not seem like a lot. However when dealing with millions of email addresses, its adds up.
- They will hijack our systems, steal our data, and hold hostage our files, again for money!

Please feel free to contact the writer of this document if you need help or advise on limiting spam. I have been using emails from a time before they were even called emails.

Prepared by: Stanley Komarniski – Headgeek
General know-it-all on technology