

INTERNET & COMPUTER SECURITY

**City of Seattle
Office of Information Security**

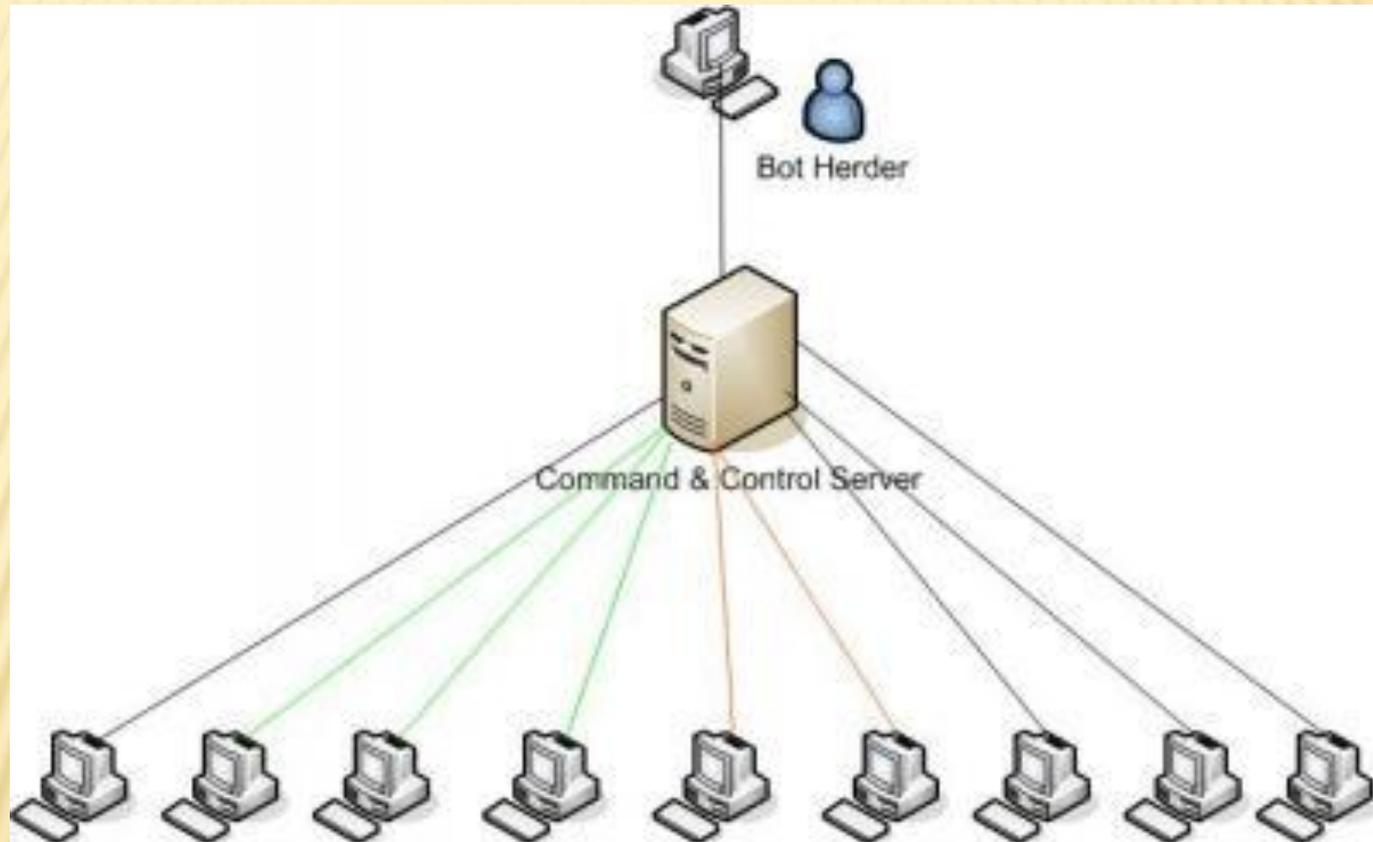


WHY IS THIS IMPORTANT?

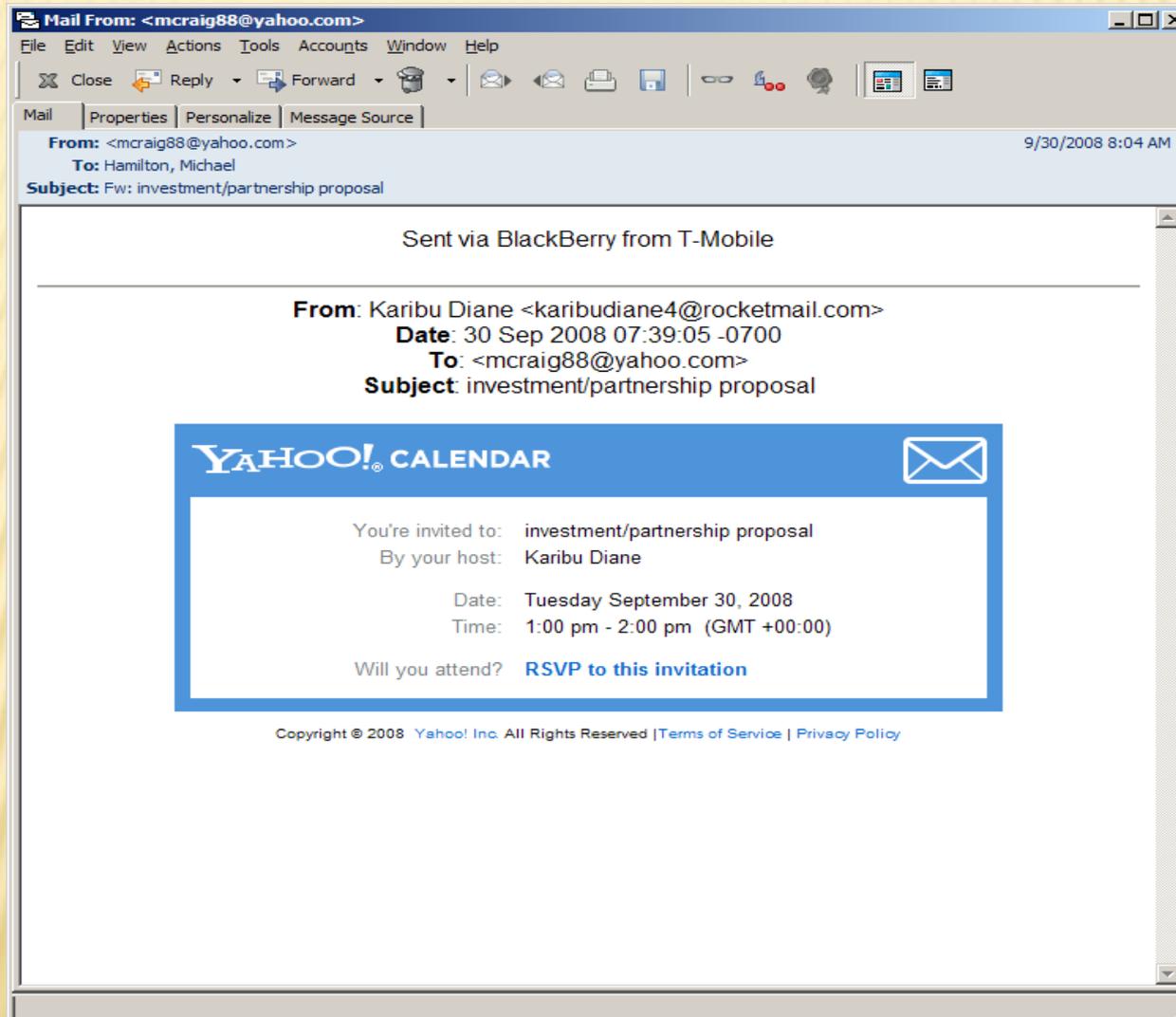
- ✘ *To The City or other organizations*
 - + Protecting Secrets and Brand Value;
 - + Avoiding Cost of Breach Reporting
- ✘ *To You, the Consumer, the Parent*
 - + Your Financial Data, Your Family
 - + Cyber Fraud surpasses physical theft - \$1.7B in losses



A “Botnet”



419 MEETING INVITATION!



The screenshot shows an email client window with the following details:

- Mail From:** <mcraig88@yahoo.com>
- To:** Hamilton, Michael
- Subject:** Fw: investment/partnership proposal
- Date:** 9/30/2008 8:04 AM

The email body contains the following text:

Sent via BlackBerry from T-Mobile

From: Karibu Diane <karibudiane4@rocketmail.com>
Date: 30 Sep 2008 07:39:05 -0700
To: <mcraig88@yahoo.com>
Subject: investment/partnership proposal

YAHOO! CALENDAR 

You're invited to: investment/partnership proposal
By your host: Karibu Diane

Date: Tuesday September 30, 2008
Time: 1:00 pm - 2:00 pm (GMT +00:00)

Will you attend? [RSVP to this invitation](#)

Copyright © 2008 Yahoo! Inc. All Rights Reserved | [Terms of Service](#) | [Privacy Policy](#)



FAKE FACEBOOK MESSAGE

Facebook Password Reset Confirmation! Your Support.

Facebook Security [customer@facebook.com]

Sent: Tue 3/23/2010 7:30 AM

To: Boone, Kathy (SCL)

Message | Facebook_password_139.zip (41 KB)

Dear user of facebook,

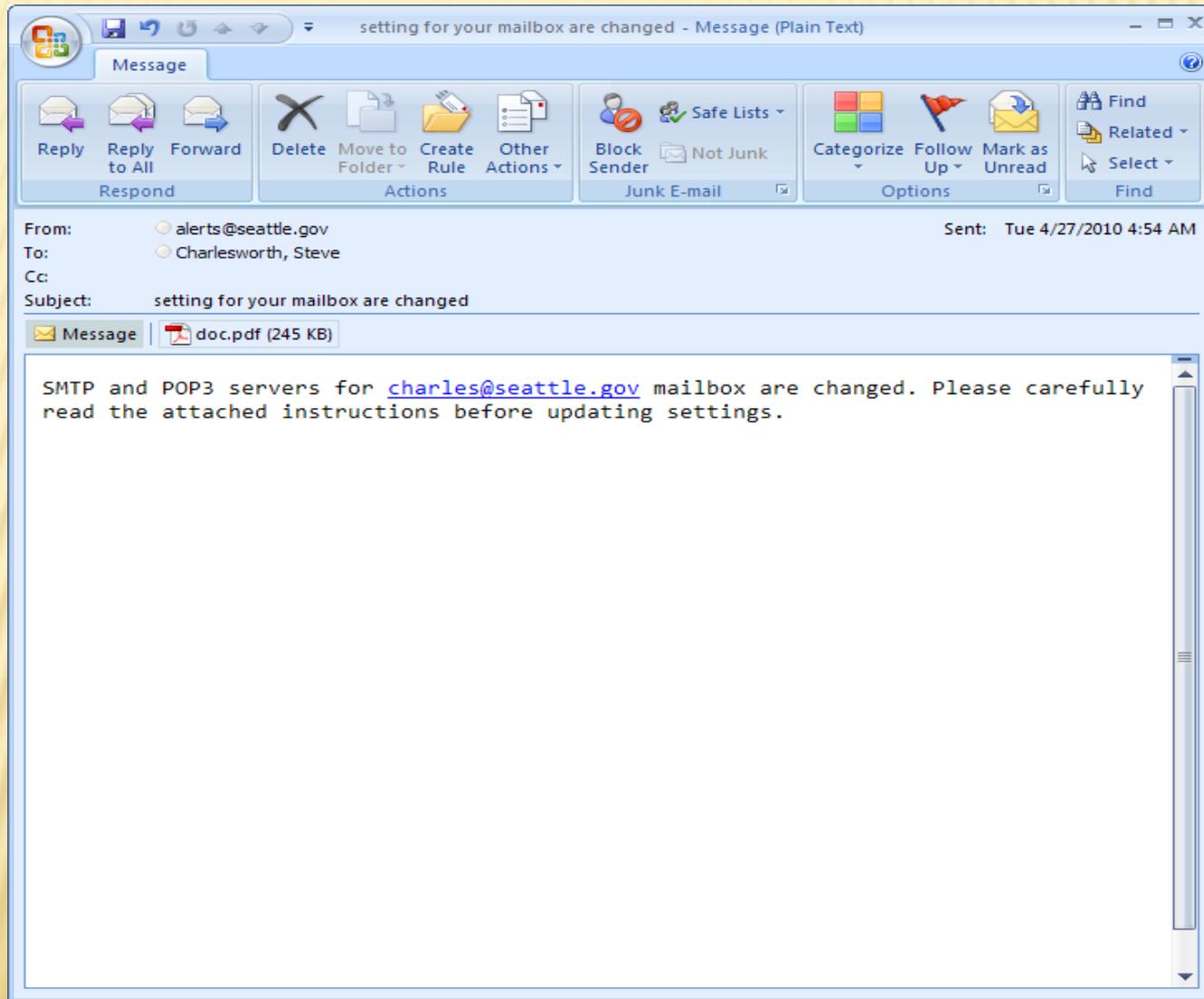
Because of the measures taken to provide safety to our clients, your password has been changed. You can find your new password in attached document.

Thanks,
Your Facebook.

All folders are up to date. Connected to Microsoft Exchange



FAKE SUPPORT MESSAGE



SELF INFLICTED INFECTIONS



BE INFORMED

- ✘ Know What's Happening IN GENERAL:
 - + Computer Security web sites
 - + Computer Magazines
 - + Software websites (Microsoft, Adobe)
 - + Government sites (FCC, NIST, DHS, FBI)
 - + Children's Safety sites
 - + Classes like this one!



BE AWARE

✘ Know What's Happening TODAY!

- Phishing, Nigerian 419 scams, Trojan du jour, social engineering, e-mail address harvesting
- Learn to Recognize Attacks in Progress
- Learn Reporting Organizations and Use Them

✘ Educate Your Kids

- MySpace, FaceBook and Other Online Communities
- Teach Suspicion



BE SUSPICIOUS

- ✘ If you get an email that seems too good to be true – it is!
- ✘ Be very cautious about unexpected email, especially if it has an attachment
- ✘ Don't follow links that you aren't sure about – or surf dangerous sites
- ✘ Don't open an attachment you weren't expecting (even if it's from a friend)



BE ALERT

- ✘ Know the types of activities to avoid
- ✘ Check for the lock symbol if you are disclosing confidential information
- ✘ Know what your kids are doing online – make rules
- ✘ Watch for symptoms
 - + Computer slow to start
 - + Applications run slowly or lock up
 - + Computer runs slow or won't shut down



BE PREPARED

Reduce Your “Attack Surface”

- ✘ Use Throwingaway E-Mail Account Information When Posting Publicly
- ✘ Hold Information Tightly
- ✘ Use “Tiered” Passwords on Websites and *change them regularly!*



TECHNICAL CONTROLS

- Automatic updates and patching
- Anti-Virus and Anti-Spyware
- Software (or “personal”) firewall
- Secure browser configuration
- Separate browser for sensitive operations
- Manage your passwords!
- Backups



STRIKING BACK

- ✘ *NEVER* Contact Scammers
- ✘ Report phishing immediately; for example phishing@paypal.com
- ✘ Also report advance-fee and pump-n-dump scammers to the e-mail service they're using
- ✘ Teach your Aunt how BCC: works



REPORTING OPTIONS

- ✘ Fraud – Federal Trade Commission (FTC.gov)
- ✘ Crimes – FBI (IC3.gov), Secret Service, Immigration and Customs Enforcement, Postal Inspection Service, Bureau of Alcohol, Tobacco and Firearms
- ✘ See <http://www.usdoj.gov/criminal/cybercrime/reporting.htm> for summary on reporting Internet crimes
- ✘ Best is www.ic3.gov for one-stop reporting



RESOURCES

- ✘ All of the above
- ✘ The Office of Information Security's website:
www.seattle.gov/informationsecurity
- ✘ Vendor sites (Microsoft, Adobe, Google, your ISP)



SUMMARY

- ✘ Your awareness and behavior is the best control
- ✘ Use good (tiered) passwords
- ✘ Understand and apply layered controls
- ✘ Be suspicious and aware
- ✘ Educate yourself and fight back!



Questions?

David R Matthews
david.matthews@seattle.gov

City of Seattle
Office of Information Security

