

Keeping Your PC Safe

Tips on Safe Computing from
Doug Copley

Don't be an Administrator

- Administrator is an account that can do ANYTHING on the PC
- Most computers start with 1 account with administrator privileges
 - Easy
 - Won't run into roadblocks trying to do something
- If a virus or hacker gets into your account, he can then do anything

Recommend:

- Note the password to the administrator account
- Create a second account as a basic user (not an administrator)
- Use the second account to do your everyday tasks
- If needed, login with the administrator account if prompted to install software, etc.

Use a Password

- **The longer, the better (12 or more is best)**
- **Uppercase, Lowercase, Numbers, Special Characters (all if possible)**
- **Easy for YOU to remember – hard for ANYONE ELSE to guess**
 - Avoid using personal information that could be guessed
 - Best if random (but makes it hard to remember initially)
 - Don't worry too much about writing it down at home
- **Can be anything you want – does not have to be a word**
- **Examples:**
 - Sr45beX_fr9P
 - My 8 yr old dog is @home
 - My wife & I bake a lot @350 degrees
 - I'm 65 years young

Use a Password Manager

- A password manager is a software application that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password which grants the user access to their entire password database.
- Most Recommended Password Managers:
 1. LastPass – Free, but premium version is \$12/yr
 2. Dashlane 4 - \$39.99
 3. Sticky Password Premium - \$14.99
 4. FREE – LastPass 4.0; LogMeOnce Password Management Suite Premium

Exercise “Safe” Behavior

- Only install applications you need
- If you didn't ask for it, don't install it!
- Once installed, update it with new patches
- When it's no longer required, remove it
- Email – don't open things from strangers
- File sharing is ok at home, but NOT on the internet
- If your PC gets infected, call A-1 in St. Clair, or use MalwareBytes on a USB stick.

Use Anti-Malware

- Antivirus/Antimalware is a MUST for every computer
- Most web email already scans your email
- Expect to pay \$20-\$40/year (some are free)

Top consumer security products:

1. Bitdefender Antivirus Plus 2017 - \$39.95
2. Kaspersky Anti-Virus (2017) - \$59.99
3. Symantec Norton AntiVirus Basic - \$19.99
4. Webroot SecureAnywhere AntiVirus (2016) - \$19.99

Top FREE consumer security products:

1. AVG AntiVirus Free (2016)
2. Avast Free Antivirus 2016
3. Panda Free Antivirus (2016)

Use a Firewall

- A firewall is like a colander
- Firewalls are strongly recommended
- Windows has one built-in
- Most anti-virus software comes with one
- Make sure it's enabled
- <Start><Control Panel>



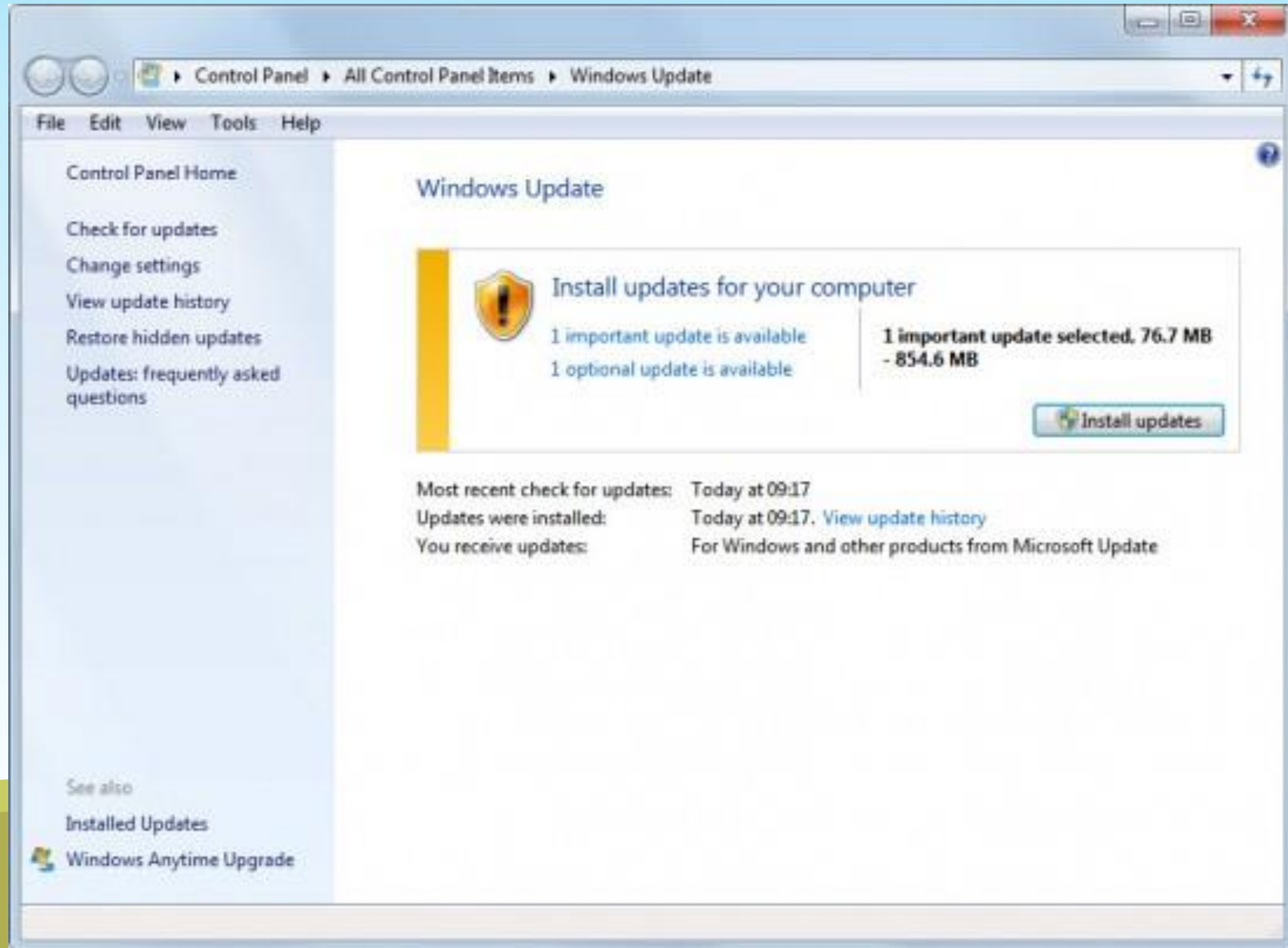
On a Mac:

1. <System Preferences>
2. <Security & Privacy>
3. Click the <Firewall> Tab
4. Enter administrator username and password
5. Click <Turn On Firewall" or <Start> to enable it

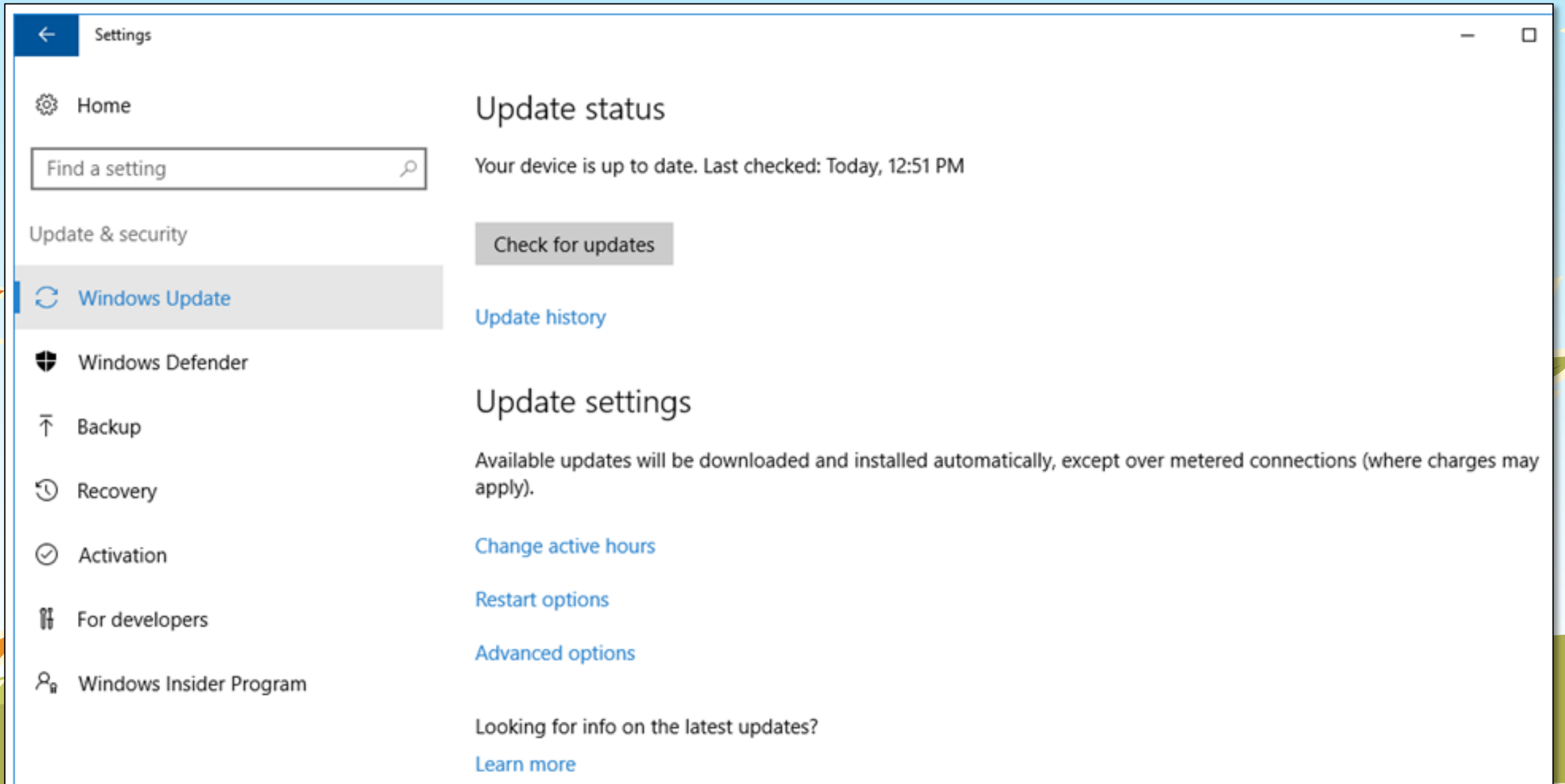
Enable Auto-Updates

- Software bugs are identified constantly (antivirus programs typically update daily)
- Criminals take advantage of the fact that companies and individuals do not perform timely updates
- Make sure auto-updates are turned on for Windows, antivirus and any programs that allow it

Windows 7 Updates



Windows 10 Updates



The screenshot shows the Windows 10 Settings application. The left sidebar contains the following settings categories: Home, Update & security, Windows Update (selected), Windows Defender, Backup, Recovery, Activation, For developers, and Windows Insider Program. The main content area is titled "Update status" and displays the message "Your device is up to date. Last checked: Today, 12:51 PM". Below this message is a "Check for updates" button. Further down, there are links for "Update history", "Update settings", "Change active hours", "Restart options", and "Advanced options". At the bottom, there is a link for "Learn more" under the heading "Looking for info on the latest updates?".

Settings

Home

Find a setting

Update & security

Windows Update

Windows Defender

Backup

Recovery

Activation

For developers

Windows Insider Program

Update status

Your device is up to date. Last checked: Today, 12:51 PM

Check for updates

Update history

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

[Change active hours](#)

[Restart options](#)

[Advanced options](#)

Looking for info on the latest updates?

[Learn more](#)

Backup Your PC Regularly





- What is ransomware?
- What if your hard drive failed tomorrow? Do you have backup copies of your documents/photos/music?
- Backups should be performed periodically
- Make sure your backup is NOT on the same computer – recommend external hard drive (or cloud)
- At least once/year make sure you try restoring something to make sure it works
- Create a boot disk in case your PC is damaged or compromised

Use a Router for Internet Access

- Internet addresses are like personal addresses (contain network address and device address)
- A wireless router is like a gatekeeper
- It also filters like a colander or firewall
- It hides your device addresses from the internet
- Strongly recommend using a router
- **CHANGE DEFAULT ADMIN PASSWORD**
- Make sure it uses WPA2 security (Do Not use WEP)
- Change default connection password if possible



Treat Personal Information Like Cash

- You're not going to give a stranger cash, right?
 - Then don't give them your personal information
 - Keep it protected – via email, web and phone
 - Only share what is needed, to whom it's needed and verify the legitimacy of the requestor
 - Don't over-share on social media (family info, location, etc.)
 - Review & restrict your privacy settings
 - If in doubt, call the company directly using a publicly available telephone number
 - If a deal is too good to be true, it's a scam!
- 
- 
- 
- 

Email Hygiene Topics

- Spam
- Phishing
- Identifying a malicious email
- Attachments
- Hyperlinks
- Should I respond or not?

Example Spam

KnowBe4
Human error. Conquered.

Live Demo:

New-school Security Awareness Training

Date: Wednesday, October 12, 2016

Time: 2:00 PM EDT

[Register Now](#)



Hi Doug,

Don't hesitate to contact me with any questions or suggestions: info@cybersecurity-excellence-awards.com

I look forward to working on this unique cybersecurity study with you!

Thank you,
Holger



Holger Schulze

Founder | Information Security Community on LinkedIn
info@cybersecurity-excellence-awards.com

[Let's Connect on LinkedIn!](#)

Sent to: Dcopley@forcepoint.com
Information Security Community, 400 E. Pratt Street, Baltimore, MD 21202, United States
Don't want future emails?
[Unsubscribe](#)

Phishing Email

- From address that LOOKS like someone you know
- Generic greeting
- Misspellings
- Link doesn't match text
- Sense of urgency
- Requires you to enter personal information or ID & Password

Example Phishing Email #1

Debit Classic Account Verification — Inbox

Delete Junk Reply Reply All Forward Print

From: Bank of America <debitcc@bankofamerica.com>
Subject: ~~Debit Classic Account Verification~~
Date: September 29, 2006 8:35:31 AM PDT
To: Michael Sheehan

Valid?

Bank of America Higher Standards

Dear Bank of America Member,

We regret to inform you, we require an immediate verification of your ~~Visa Debit Classic~~ card because we have reasons to believe that your account may have been compromised by outside parties.

Sense of urgency

In order to protect your sensitive information, we temporarily suspended your account for further investigations.


To reactivate your account and verify your Visa Debit Classic, click on the encrypted link below and confirm your identity by completing the secure form that will appear:

<http://www.bankofamerica.com/state.cgi?section=signin>

The link pointed to <http://debitcc.bankofamerica.uo-s.com/xxxx>

Take our apologies for any inconvenience that this may cause.

Thank you,
Bank of America Internet Banking.

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 
© 2006 Bank of America Corporation. All rights reserved.

Link to real web site

Example Phishing #2

From: PayPal <Payment-notify@mail.com>
Date: Thursday, August 11, 2016
Subject: You received a payment from your buyer - Ship now
To: [REDACTED]

PayPal

Transaction ID: [4DN42501R7813401J](#) | Transaction Time: 08/11/2016

You received a payment from your buyer - Ship NOW

Dear [REDACTED]

You've received a payment of \$1,845.00 USD from Zion for your recent eBay sale.

Estimated funds availability

While you establish a successful eBay sales history, you may not have access to your money for up to [21 days](#). You may [get it sooner](#), but it may take longer if your buyer reports a problem with the sale.

NOTE: This PayPal payment has been deducted from the buyer's account and has been "APPROVED" but will remain PENDING until the shipping tracking number is sent to our customer service for shipment verification so as to secure both the buyer and the seller

Annotations:

- Valid? mail.com? (points to the sender email)
- Bogus ID (points to the transaction ID)
- Legitimate PayPal Links (points to the transaction ID)

Help get your money faster

- Print [eBay](#) or [PayPal](#) labels so your tracking information uploads automatically
- Manually enter your [tracking information](#) on eBay or send PayPal the tracking number for verification, if you ship domestically directly through USPS, UPS, or FedEx
- Email us the shipping tracking number via membership_safety@mail.com
- [Mark your items](#) as shipped on eBay

Buyer
Zion Kally
ZionKally00900906@yahoo.com

Shipping address - Confirmed
Laura Toledo, Box 1292 Cuba New Mexico 87013 USA

Note to seller
Please i want it mail via [USPS Express mail](#)

Seller Protection Eligible

Description	Purchase Date	Unit price	Qty	Amount
[NEW] Microsoft Surface Book - Intel Core i5 6th Gen 256GB 8GB dGPU Item# 322224401956	August 11 2016	\$1,845.00 USD	1	\$1,845.00 USD

Selling Legitimacy (points to the item description)

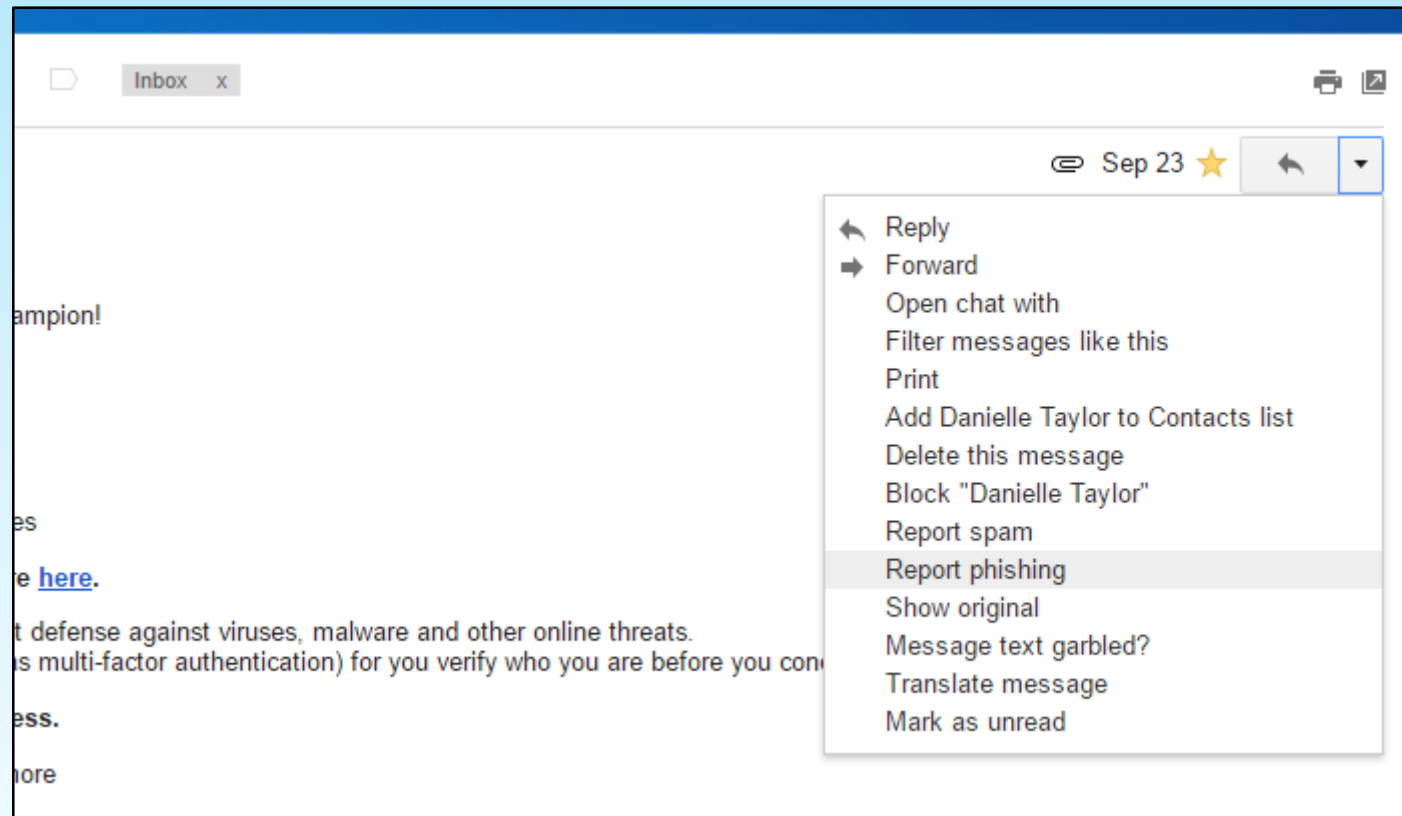
Sense of Urgency (points to the note to seller)

Subtotal	\$1,795.00 USD
Shipping and handling Insurance - not offered	\$50.00 USD
Tax	
Total	\$1,845.00 USD

Annotations:

- Suspicious Email (points to the buyer's email)

Reporting Spam & Phishing in Gmail



To report a potentially malicious or abusive Gmail user, go to

<https://support.google.com/mail/contact/abuse>

Email Hygiene

- Don't OPEN attachments you weren't expecting
- DO NOT click on hyperlinks unless you KNOW you can trust them
- Reply or Not Reply...That is the Question
 - They may be validating your email is legitimate – Don't
 - In general, delete unless unsubscribing to spam
- Unsubscribing
 - Compliant companies must allow you to unsubscribe to an email list in 2 clicks or less
 - Recommend doing for spam



Thank You!

Email: copleydt@yahoo.com

Twitter: @copleydt

LinkedIn: www.linkedin.com/in/dcopley

