3 Ways to Avoid the Computer Repair Guy

with Ben Hayes

SPARK ZONE

ben.hayes@sparkzoneiowa.com
www.sparkzoneiowa.com

Who am I?

GREATNESS STEMS FROM IOWANS

Class Outline

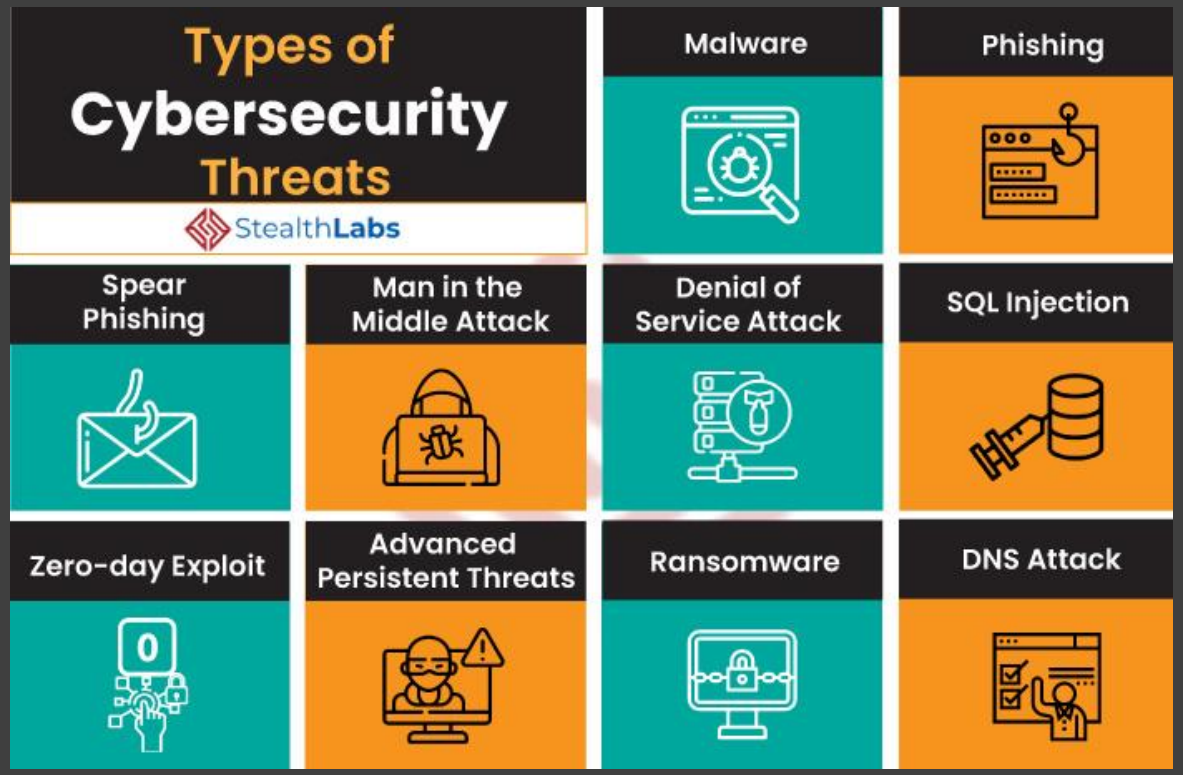
- Section 1 – Cyber Security Overview
- Section 2 – Protect Yourself
- Section 3 – Protect Your Device
- Section 4 – Protect Your Data

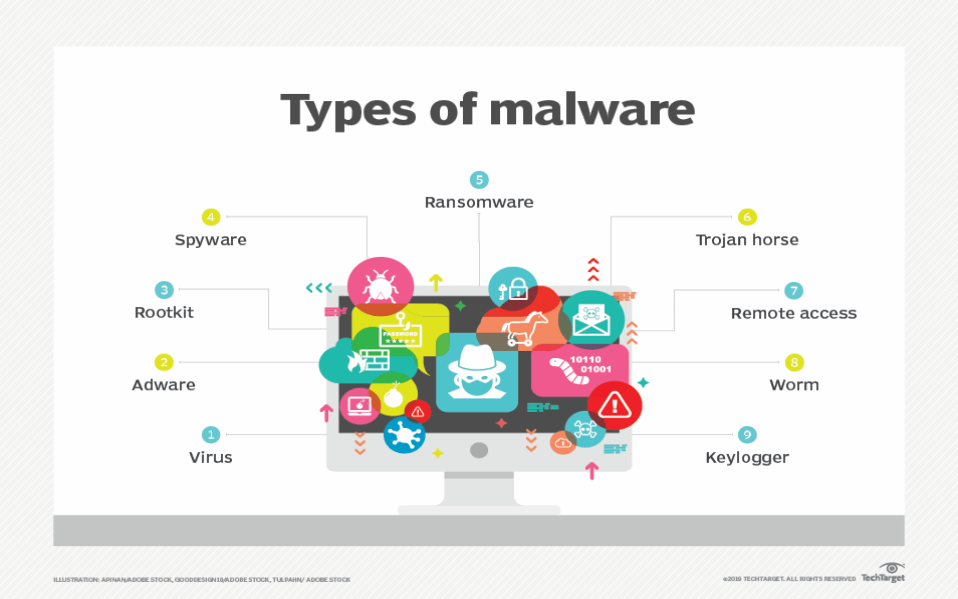
Section 1:
Cyber Security Overview

- Types and Threats
- Trends and Stats

Types and Threats

- Malware
- Phishing





Malware

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

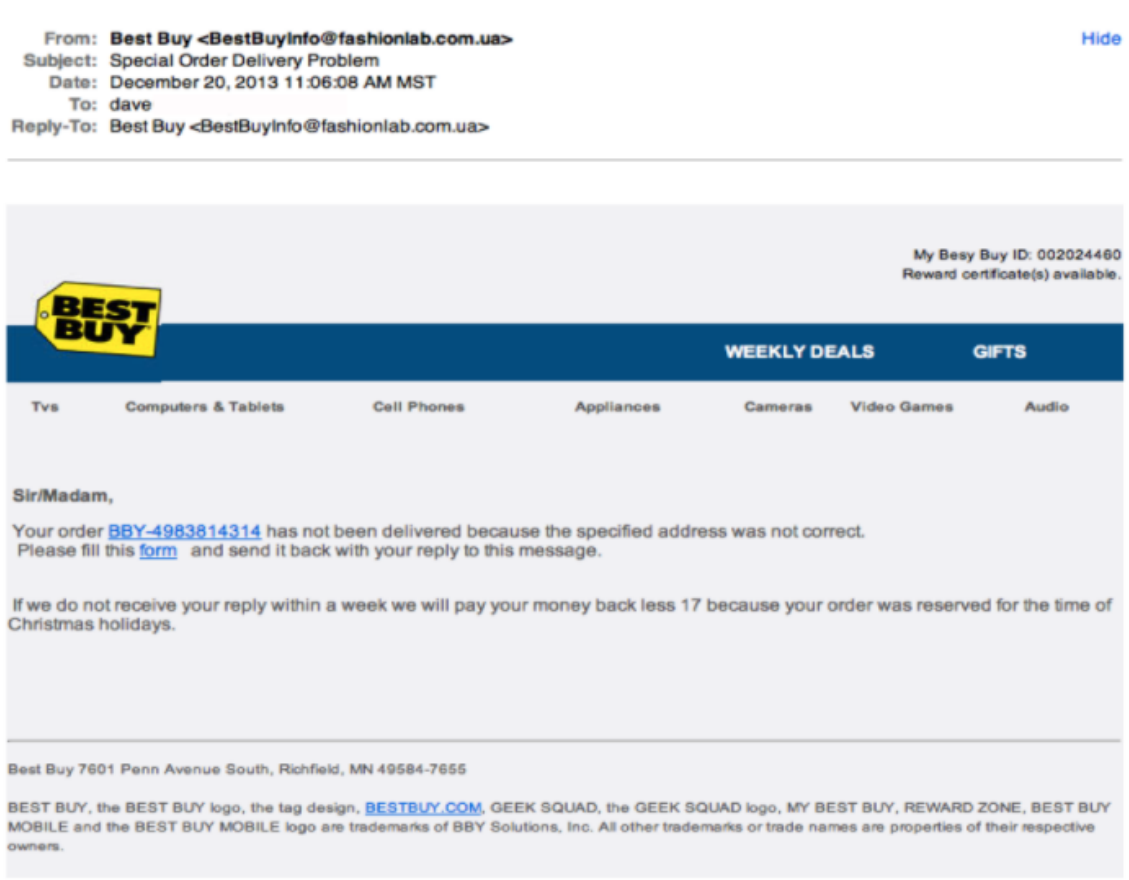
Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware.

- ❑ Ransomware
  - Encrypts a victim's data and prevents access until a ransom payment is made
- ❑ Scareware
  - An attack that claims to have detected a virus or other issue on a device and directs the user to download or buy malicious software to resolve the problem.

Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.



From: Best Buy <BestBuyInfo@fashionlab.com.ua>
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

Hide

My Besy Buy ID: 002024460
Reward certificate(s) available.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

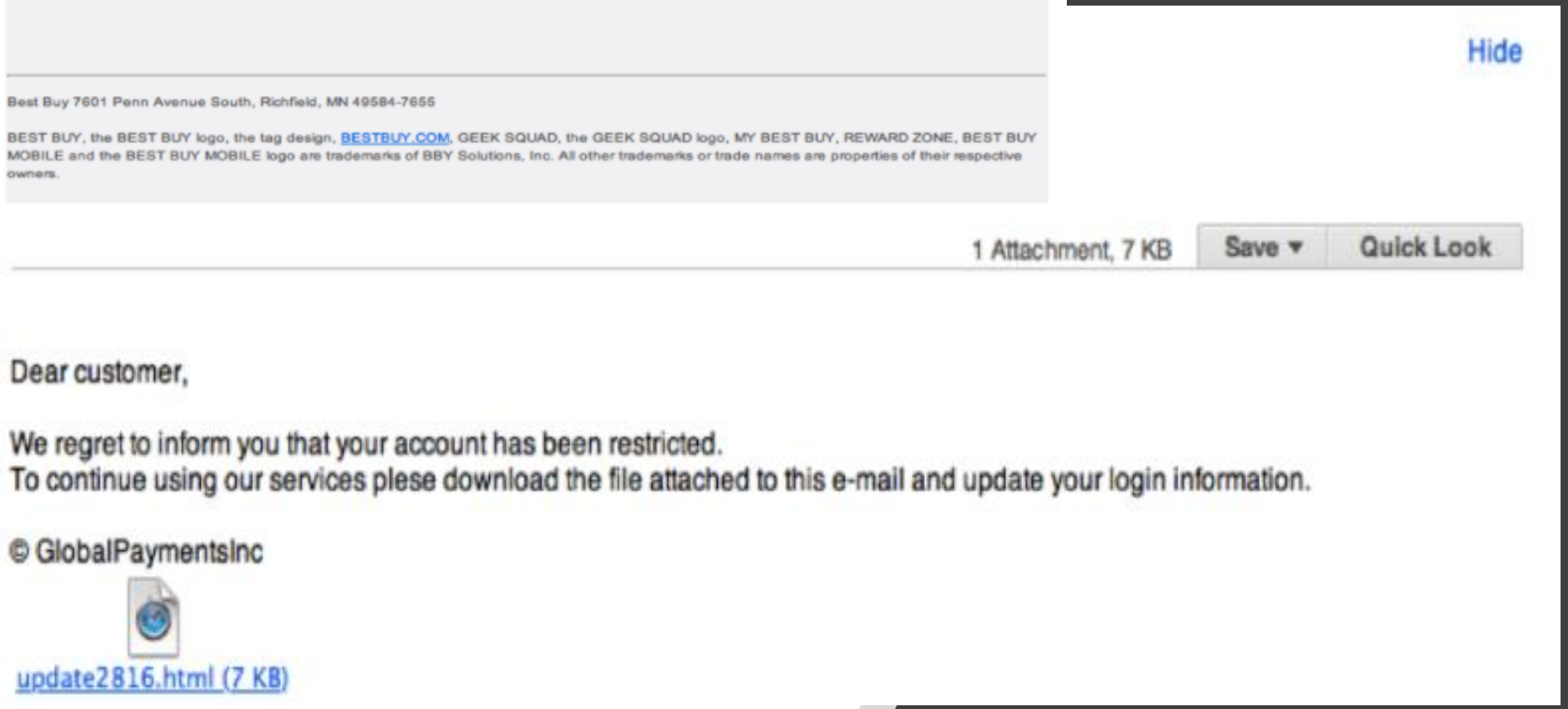
Sir/Madam,

Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, BESTBUY.COM, GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.



Hide

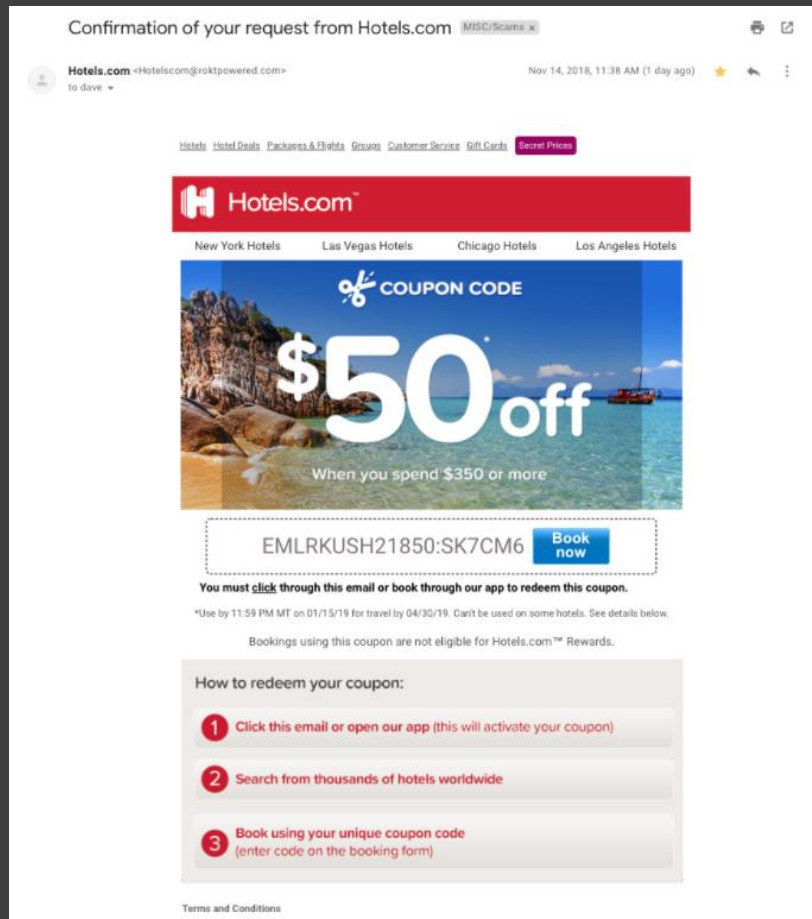
1 Attachment, 7 KB Save ▾ Quick Look

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)



Confirmation of your request from Hotels.com MISC/Scams

Hotels.com <Hotelscom@roktpowered.com> Nov 14, 2018, 11:38 AM (1 day ago)
to dave

Hotels Hotel Deals Packages & Flights Groups Customer Service Gift Cards Secret Prices

Hotels.com

New York Hotels Las Vegas Hotels Chicago Hotels Los Angeles Hotels

COUPON CODE

$50 off

When you spend $350 or more

EMLRKUSH21850:SK7CM6 Book now

You must click through this email or book through our app to redeem this coupon.

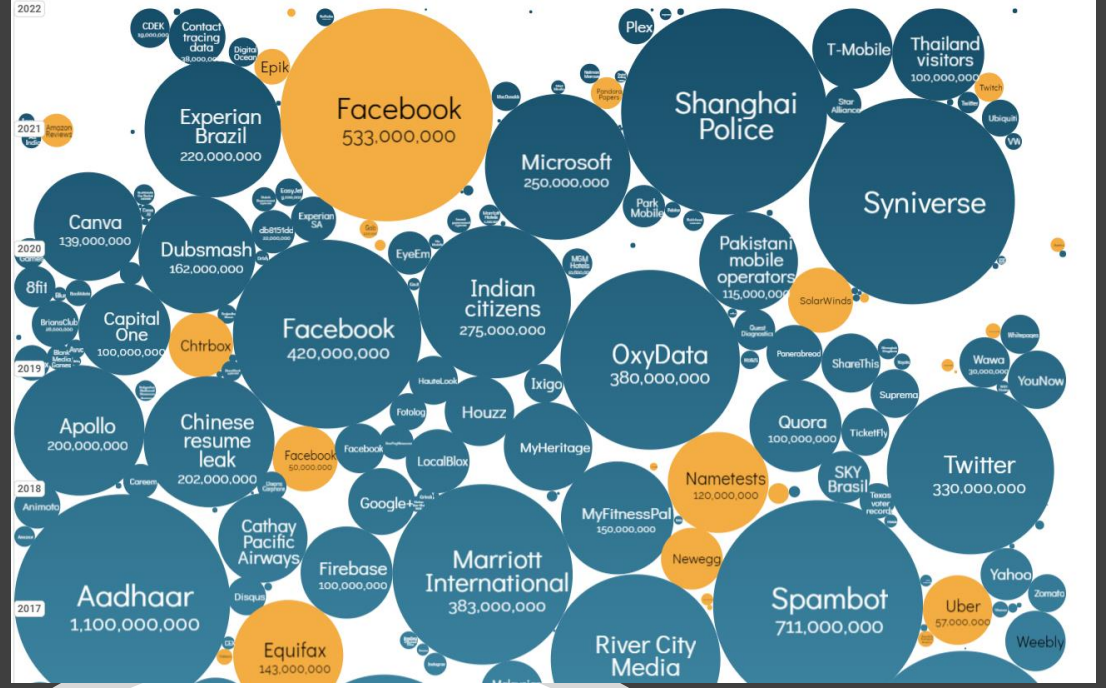
*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

Bookings using this coupon are not eligible for Hotels.com™ Rewards.

How to redeem your coupon:

1. Click this email or open our app (this will activate your coupon)
2. Search from thousands of hotels worldwide
3. Book using your unique coupon code (enter code on the booking form)

Terms and Conditions



Trends and Stats

- The global average cost of a data breach is USD 3.92 million
- Cybercrime breaches to increase by 76% by 2024
- Over 50% of all global data breaches to occur in the United States by 2023
- The average cost of a data breach to a US company is USD 7.91 million
- The average number of days to identify an incident is 206 days
- Cyberattacks on IoT devices increased by 300%
- Data breaches exposed 22 billion records in 2021
- The top malicious email attachment types are .doc and .dot which make up 37 percent; the next highest is .exe at 19.5 percent

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Section 2:
Tip #1 – Protect Yourself

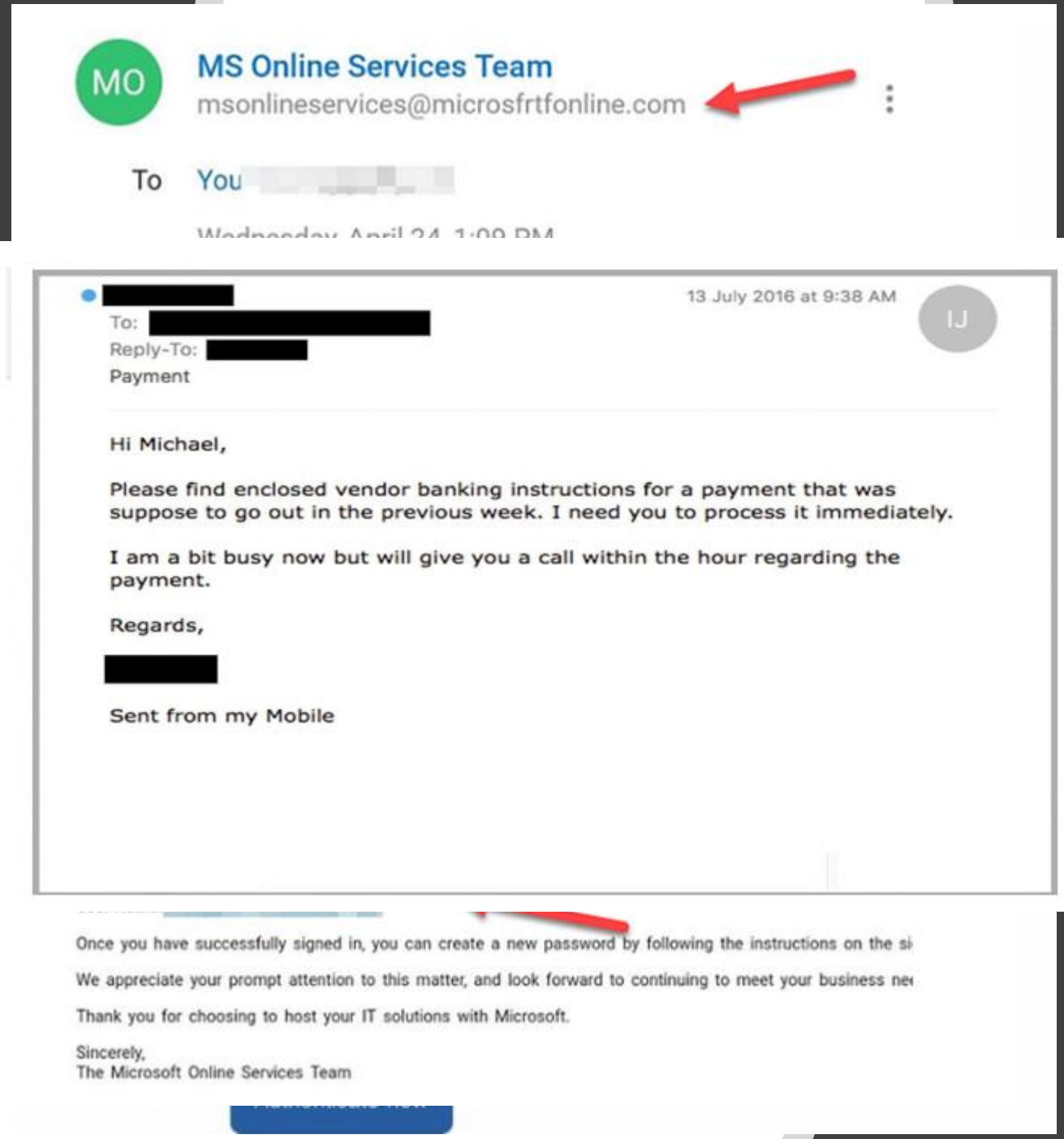
- Password Practices
- Phishing Awareness
- Scareware Awareness
- Account Health Check
- Tools to Help

Password Practices

- ❑ Passphrase
  - Still just a password, but longer
  - Most likely a sentence
  - Includes upper-case and lower-case letters and punctuation
  - Much more secure than a shorter password with more complexity
- ❑ Strong Passwords
  - Not easy to guess
  - Length is more important than complexity
  - Effective password should be no less than 14 characters
  - Don’t share passwords with other accounts
- ❑ Multi-Factor Authentication
  - Prevents password guessing or brute force attacks
  - Requires more authentication to gain access

https://www.security.org/how-secure-is-my-password/

Phishing Awareness



MO

MS Online Services Team
msonlineservices@microsfrtfonline.com

To You

[redacted]
To: [redacted]
Reply-To: [redacted]
Payment

13 July 2016 at 9:38 AM

IJ

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

- The message is sent from a public email domain
- The domain name is misspelled
- The email is poorly written
- It includes suspicious attachments or links
- The message creates a sense of urgency

Scareware Awareness

- Never click links or download files from pop up ads or unfamiliar email senders.
- Install a pop-up blocker and spam filter which will detect many threats and even stop scareware pop up ads and infected emails from reaching your device.
- Invest in cybersecurity software from a reputable antivirus vendor and ensure all installations are up to date.
- Log into your account through a new browser tab or official app—not a link from a scareware alert, email or text message.
- Only access URLs that begin with HTTPS.
- Never share personal information, such as account numbers, passwords or credit card details, via phone, email or unsecured site.

';--have i been pwned?

Account Heath Check

Check your account health frequently as breaches happen all the time.

- Check if your email has been exposed in the Dark Web
https://haveibeenpwned.com/

- Check if your passwords have been exposed
https://haveibeenpwned.com/Passwords

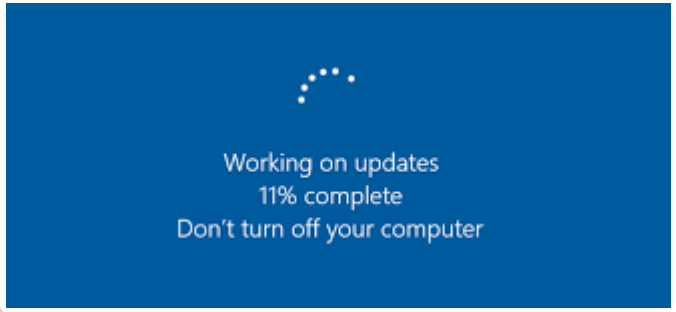
Tools to Help

These tools can help protect you and make life online a lot easier to manage.

- LastPass – www.lastpass.com
- AdBlocker Plus - adblockplus.org

Section 3:
Tip #2 - Protect Your Device

- Software Updates
- Locking Your Devices
- Remove Unwanted Applications
- Malware Protection



Software Updates

Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software program or operating system.

Hackers can take advantage of the weakness by writing code to target the vulnerability. The code is packaged into malware.

An exploit sometimes can infect your computer with no action on your part other than viewing a rogue website, opening a compromised message, or playing infected media.

Locking Your Device

Mobile technology allows us to perform many tasks while we are on the go, from online banking and shopping to emailing.

Mobile security is important as our smartphones hold a lot of sensitive data. Locking your phone is a simple security step, yet many people don’t use a screen lock.

Generally, you should always lock devices that have sensitive data on them. This includes computers, mobile devices, and tablets.

Most devices have a setting that will automatically lock your device after a certain period of inactivity. This is especially beneficial if you tend to forget to lock your computer.

If you’re on a mobile device, you may be able to restrict or lock individual apps through the settings on your phone.

Remove Unwanted Applications

Old apps that no longer get updates or that you haven't updated in some time because you never use them can harbor serious security flaws.

Malware Protection Tips

- Ensure you have anti-virus running on your device
- Use an email system that help filter out spam and potentially malicious links and downloads
- Use pop-up blockers and other add-ins that anti-viruses won’t stop
- Use multi-factor authentication (MFA) whenever possible

Section 4:
Tip #3 – Protect Your Data

- Backups
- Internet Data
- Secure Browsing

Backups

Backup software offers protection for data by copying desktops and laptops, and other devices in case of user error, malicious attack, corrupt files, or a physical disaster that renders personal data inaccessible.

CARBONITE®

https://www.carbonite.com/

Internet Data

HTTP cookies are essential to the modern Internet but a vulnerability to your privacy. Cookies let websites remember you, your website logins, shopping carts and more.

Removing cookies can help you mitigate your risks of privacy breaches. It can also reset your browser tracking and personalization.

Removing normal cookies is easy, but it could make certain web sites harder to navigate. Without cookies internet, users may have to re-enter their data for each visit.

Secure Browsing

- Incognito Mode - In Incognito, none of your browsing history, cookies and site data, or information entered in forms are saved on your device.
- VPN’s - Hide your internet activity and location to avoid being tracked (especially on public WiFi networks).
- Anonymous Browsing – Use Tor Project Browser and VPN to help hide your identity.

https://www.expressvpn.com/
https://www.torproject.org/download/

Section 4: Conclusion

- Protect Yourself
- Protect Your Device
- Protect Your Data