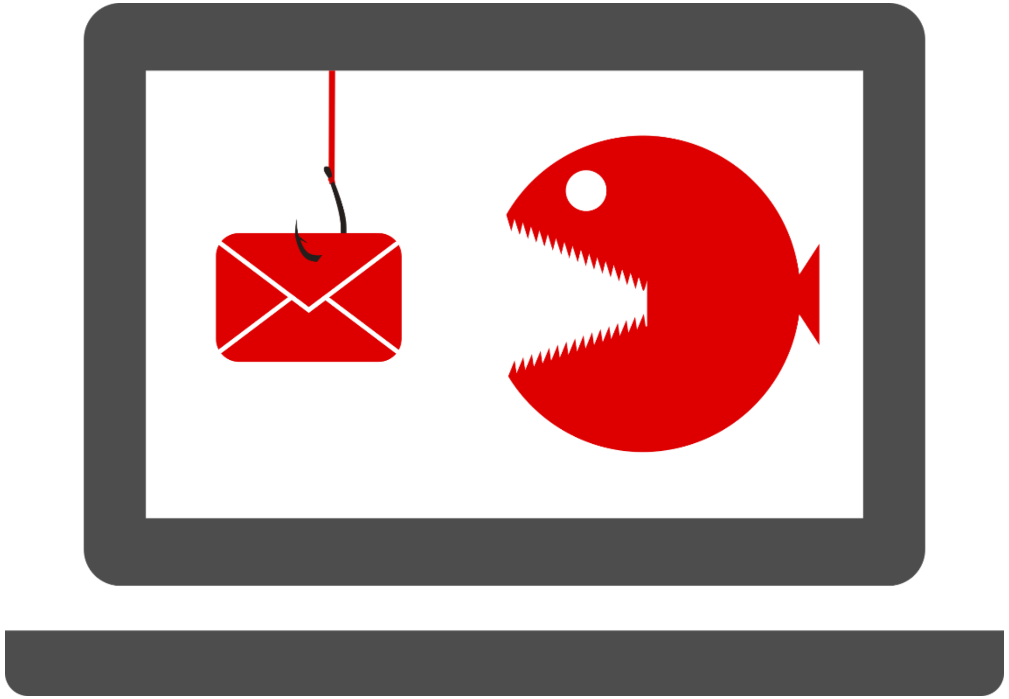
Phishing & Email



QUESTIONS? EMAIL US: INFO@HAMDENLIBRARY.ORG

PDF AVAILABLE AT: HTTP://HAMDENLIBRARY.ORG/COMPUTERLAB

What is Phishing?

“Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.” (Source: Wikipedia)

Primarily attempted through email messaging, but can also be through text, phone or phony websites.

Criminals often pretend to be an organization you trust, like banks, online retailers, government agencies and more.

Often the emails are designed to look as authentic as possible.

Types of Phishing and related scams

Phishing: regular phishing is done through email and typically targets many people at once

Smishing: phishing scams conducted over SMS (Short Message Service) text messages

Vishing: “Voice Phishing” phishing scams conducted over the phone

Spear Phishing: phishing attacks targeted at a single individual or organization

Pharming: directing users to malicious websites using DNS ‘Poisoning’

Clone Phishing: a variant of phishing where the attacker uses a copy of a previously sent message and changes or inserts a malicious link inside of it.

Whaling: phishing targeting high-profile businesses, CEO’s and politicians

Spam vs Phishing

Despite both being annoying and unwanted, spam is not necessarily phishing and phishing is not necessarily spam.

Spam is an unsolicited email message sent in bulk to a large number of recipients

Spam can be used to distribute phishing messages, but can also include benign advertisements for businesses

In the United States certain types of spam are illegal thanks to the CAN-SPAM Act of 2003.

If an unsolicited email is primarily commercial (advertising) in purpose, or contains false/misleading information in the From/Subject/Address information it is considered illegal.

Businesses are also legally required to stop emailing you if you unsubscribe/ask them to stop.

Illegal Spam can be reported to the U.S. Federal Trade Commission by forwarding the spam message to **spam@uce.gov**

What should I look for in a Suspicious Email?

Is the spelling/grammar/word choice very poor or weird?

Is the greeting very generic “Dear Sir/Madam”?

Does it imply severe negative consequences if you don’t follow its instructions immediately?

Is the email too good to be true (win a prize for a contest you never entered for instance)?

Does it demand personal information?

Are the URLs in links in the email mismatched?

Is the URL/Email address misspelled or out of order?

If the message was unsolicited does it ask you to open an attachment of some kind?

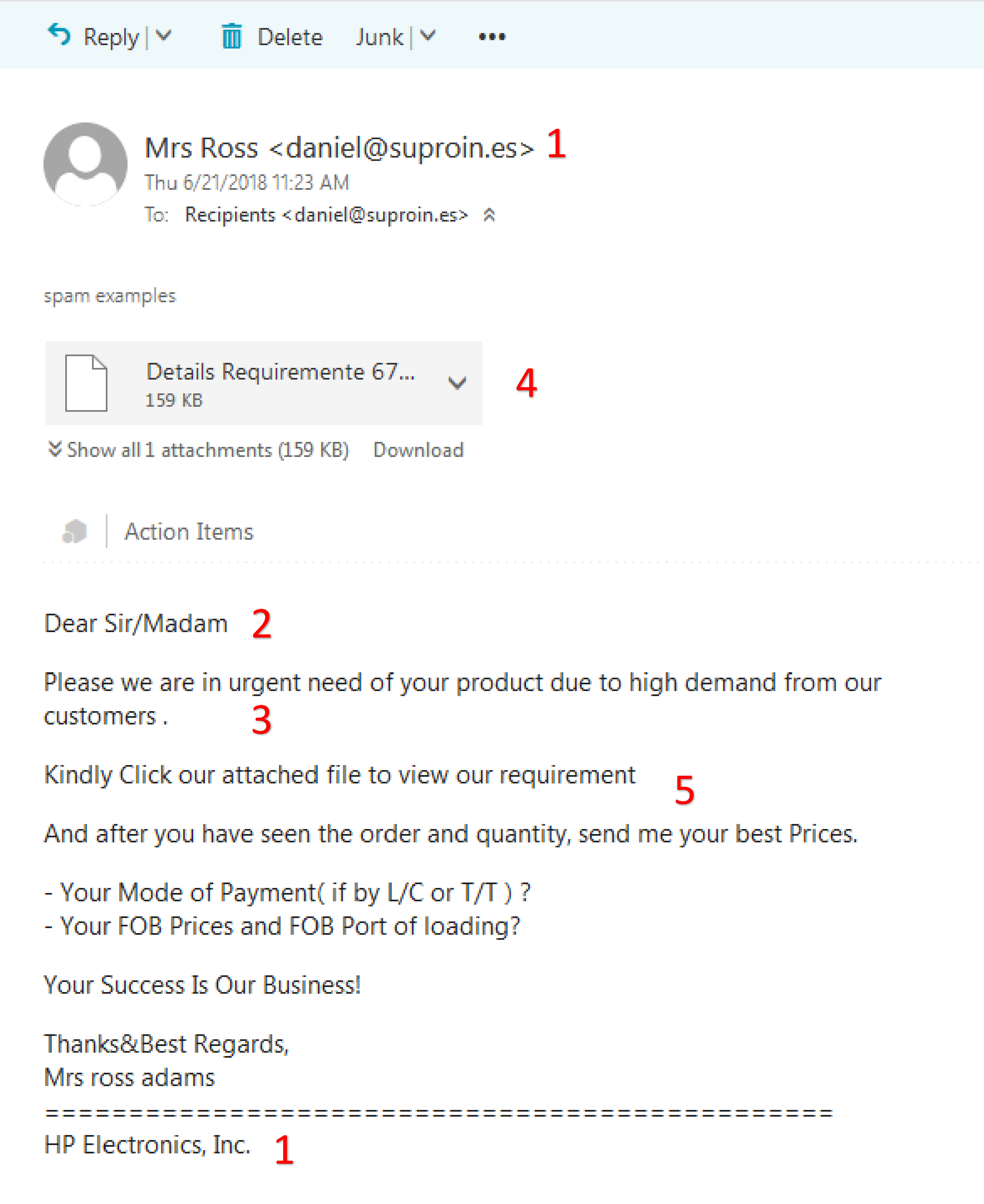
In general, always be suspicious when it comes to email and the internet, especially if it is trying to frighten/entice you.

What does a Phishing Message Look Like

An example of a scam email

This one has several problems with it:

1. Email domain is @suproin.es whereas the email is supposedly from HP Electronics, a very well known company at that
2. The greeting is an extremely generic “Dear Sir/Madam” if they were a customer they should know your name.
3. Tries to hurry you into acting without thinking by saying they are in “urgent need”
4. Trying to get you to open an unknown attachment
5. Poor formatting and grammar



Mrs Ross <daniel@suproin.es> 1
Thu 6/21/2018 11:23 AM
To: Recipients <daniel@suproin.es>

spam examples

Details Requiremente 67...
159 KB 4

Show all 1 attachments (159 KB) Download

Action Items

Dear Sir/Madam 2

Please we are in urgent need of your product due to high demand from our customers . 3

Kindly Click our attached file to view our requirement 5

And after you have seen the order and quantity, send me your best Prices.

- Your Mode of Payment(if by L/C or T/T) ?
- Your FOB Prices and FOB Port of loading?

Your Success Is Our Business!

Thanks&Best Regards,
Mrs ross adams
==
HP Electronics, Inc. 1

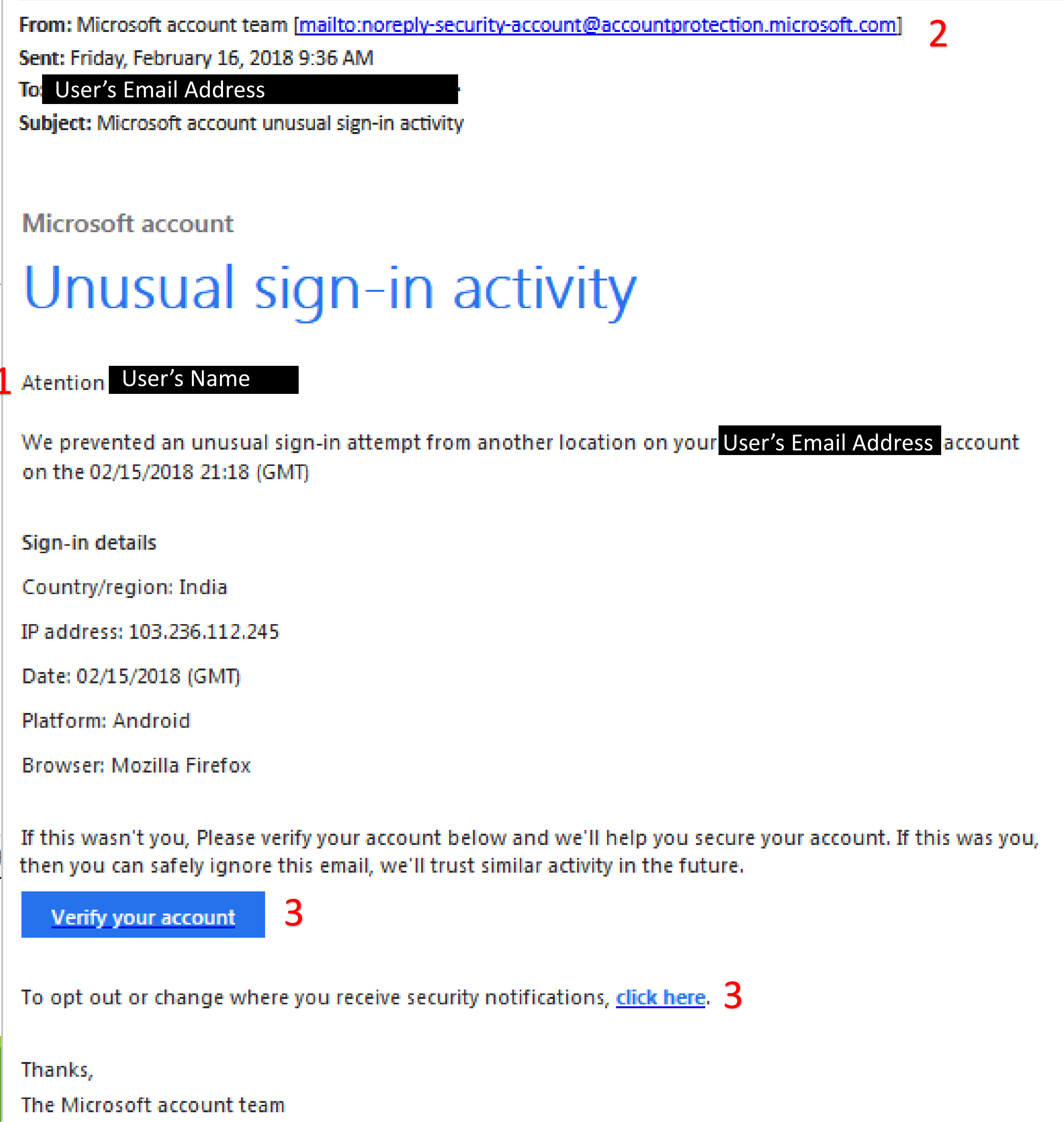
Another Example Phishing Email

This email is a pretty good phishing attempt, but it has some problems with it

1. Grammar/Spelling: most businesses proofread their emails before sending them out, this one has several mistakes in it (‘Atention’ being the most obvious).

2. The from email address is a spoof of the real Microsoft security email which is: account-security-noreply@accountprotection.microsoft.com They swapped the first part of the email around to look convincing

3. The “Verify” & “Opt out” links both lead to the same web address, www2microsoftonline.xara.hosting/secure/pvt/43a9f9f1b9 The real Microsoft site is microsoft.com/, this one is xara.hosting. You can see the URL by moussing over the buttons or links in the email



From: Microsoft account team [mailto:noreply-security-account@accountprotection.microsoft.com] 2
Sent: Friday, February 16, 2018 9:36 AM
To: User’s Email Address
Subject: Microsoft account unusual sign-in activity

Microsoft account

Unusual sign-in activity

1 Atention User’s Name

We prevented an unusual sign-in attempt from another location on your User’s Email Address account on the 02/15/2018 21:18 (GMT)

Sign-in details

Country/region: India

IP address: 103.236.112.245

Date: 02/15/2018 (GMT)

Platform: Android

Browser: Mozilla Firefox

If this wasn't you, Please verify your account below and we'll help you secure your account. If this was you, then you can safely ignore this email, we'll trust similar activity in the future.

To opt out or change where you receive security notifications, click here. 3

Thanks,
The Microsoft account team

What do they want you to do?

Phishing emails are often trying to do one of two things: open an infected attachment or follow a link to a website

Phishing emails with attachments:

- The attachment will usually contain malware of some kind that will try to infect your computer.
- What type of malware varies, it can spy on you, record passwords you type in to other sites, install ransomware or all sorts of other stuff.

A link to a website

- In this case the hacker will most likely have set up a phishing website designed to trick you into entering in a password to an online account so they can steal it.
- These sites will often try to imitate the look of the legitimate website they are copying.
- Never follow the link in an email to go to a site, enter the address yourself, either in the URL bar or in a search engine.
- If you accidently click on the link and end up at a phishing website all is not lost; do not click on anything in the website and use the back button on your browser to leave (or close the tab you are on). If you are still worried afterward have your antivirus preform a scan of your system.

Deceptive URLs

When dealing with links to websites in phishing emails, scammers will typically try to trick you in one of two ways (and sometimes will combine these two together)

Spoofed URL: the attacker will attempt to make the URL look like the one used by the website they are pretending to be

Real website	https://myaccount.google.com/
Fake website	https://myaccount.gooogle.com/
Fake website	https://myaccount.google.com.rekcahami.win/
Fake website	data:text/html,https://myaccount.google.com/

Deceptive URL Hyperlink: sometimes the link in the email will say one thing but do another

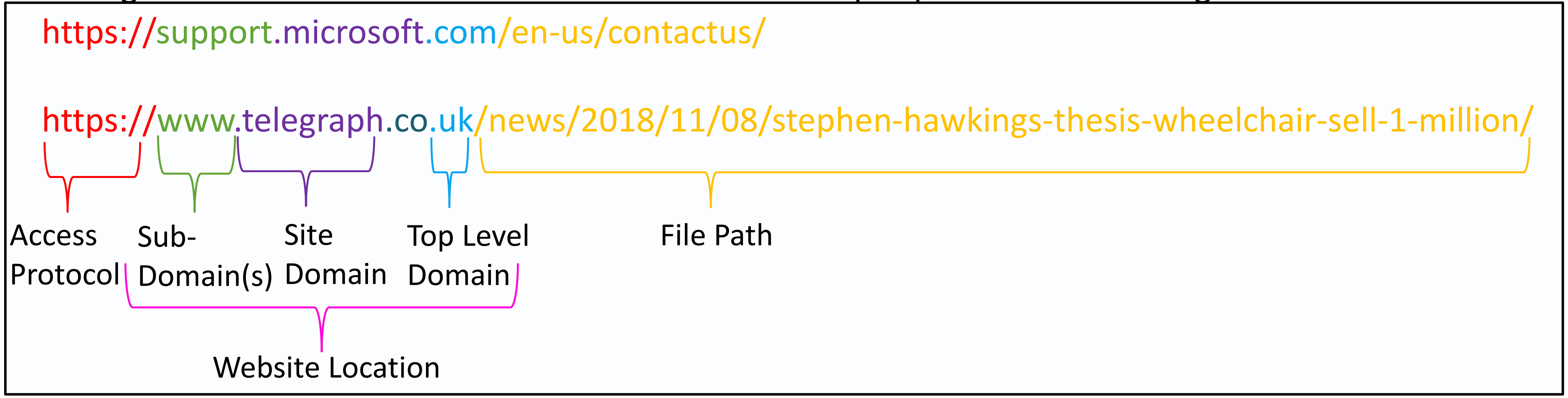
- Here we have a URL that supposedly links to google.com but really goes to another site:
- http://www.google.com/
- By hovering over the link in an email, a tooltip should appear either next to your cursor or in one of the bottom corners of the window that reveals the actual address link.

Also be aware that attackers can use non-Latin letters to make URL's appear identically, to a company's website, https://www.xn--80ak6aa92e.com/ for example appears as https://www.apple.com/ in Firefox.*

*To make Firefox display the right URL, go to **about:config** in the address bar, agree to the warning, search for **Punycode,** find **network.IDN_show_punycode** and change it to **True**

Uniform Resource Locator (URL)

Knowing the basics of how to read a website’s URL is very important for avoiding scams on the internet



https://support.microsoft.com/en-us/contactus/

https://www.telegraph.co.uk/news/2018/11/08/stephen-hawkings-thesis-wheelchair-sell-1-million/

Access Protocol

Sub-Domain(s)

Site Domain

Top Level Domain

File Path

Website Location

- Top Level Domain: Highest level organization can be generic e.g. .com .org .net or country specific .uk (sometimes a second level domain is included with country codes, .co.uk means a commercial site in the United Kingdom)
- Site Domain: identifies the name of the website that you want to visit
- Sub Domain: usually used for denoting different parts of a website. A website can have many subdomains
- Protocol: tells how a website is being accessed, HTTPS is preferred due to its secure connection
- File Path: The location of a particular webpage or file within a website

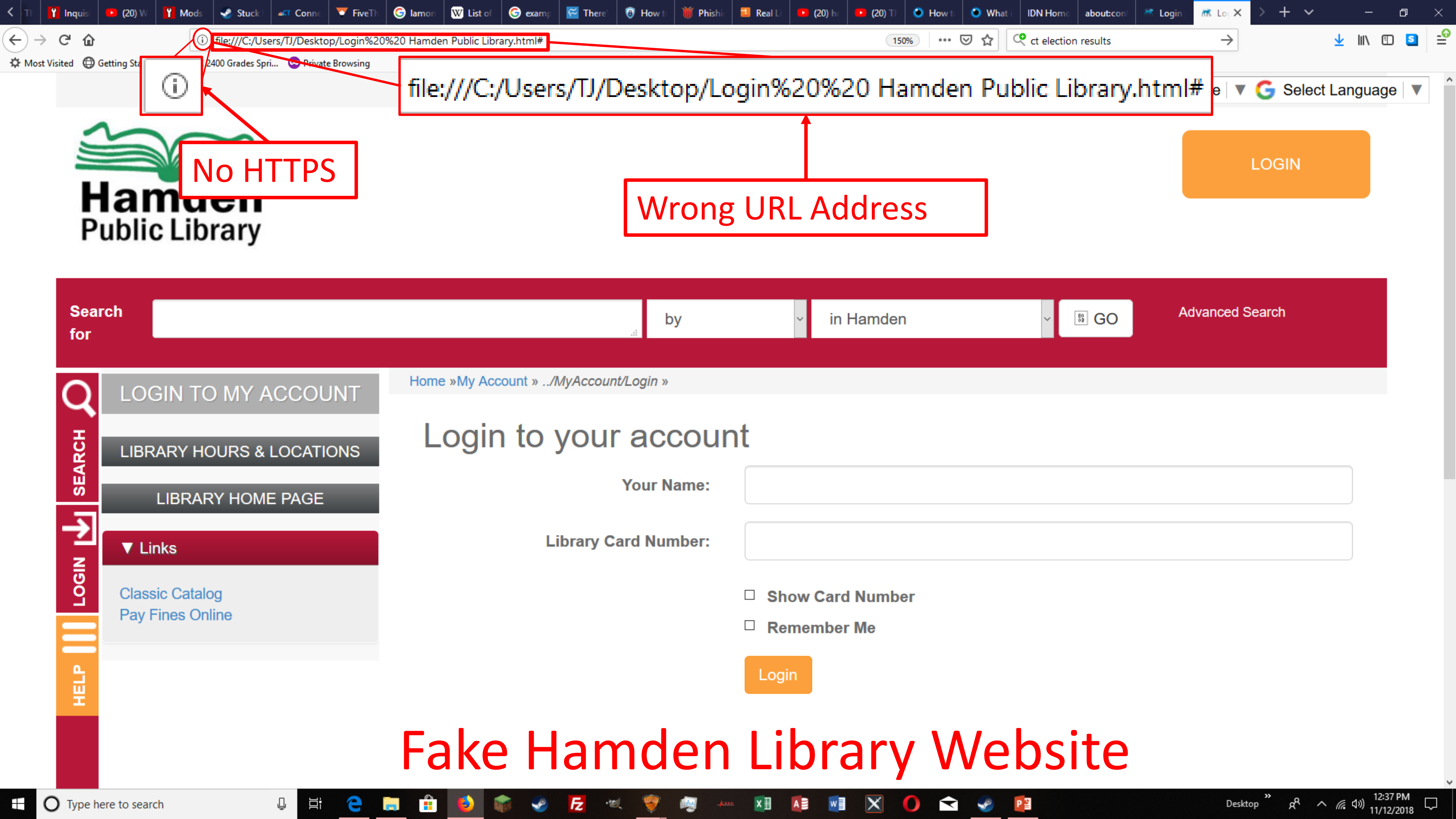
Phishing Websites

What do they look like?

- Many times the phishing email will send you to a phishing website made to look like the original
- Typically it will be a login page asking for your username and password (or credit card information).
- Entering your information into the site will usually result in an error message and might even send you to the real website once it has your data.
- The phishing website will have logged the information you entered into a file that the attacker can harvest the data from.
- It is very easy to copy (clone) a website in order to make a phishing site, very convincing fakes can be made in a few hours or days.

The ways of spotting a fake website are very similar to spotting a fake email with the most important being:

- Look carefully at the URL and make sure it is correct.
- Is the site HTTPS? **Having HTTPS is not a guarantee that a site is legitimate**, but not having HTTPS, especially when a site is asking for personal information is a sign that it is a scam.
- Is the spelling/grammar very poor?
- Are the prices/terms/offers too good to be true?



file:///C:/Users/TJ/Desktop/Login%20%20 Hamden Public Library.html#

No HTTPS

Wrong URL Address

Hamden Public Library

LOGIN

Search for

by

in Hamden

GO

Advanced Search

Home »My Account » ../MyAccount/Login »

Login to your account

Your Name:

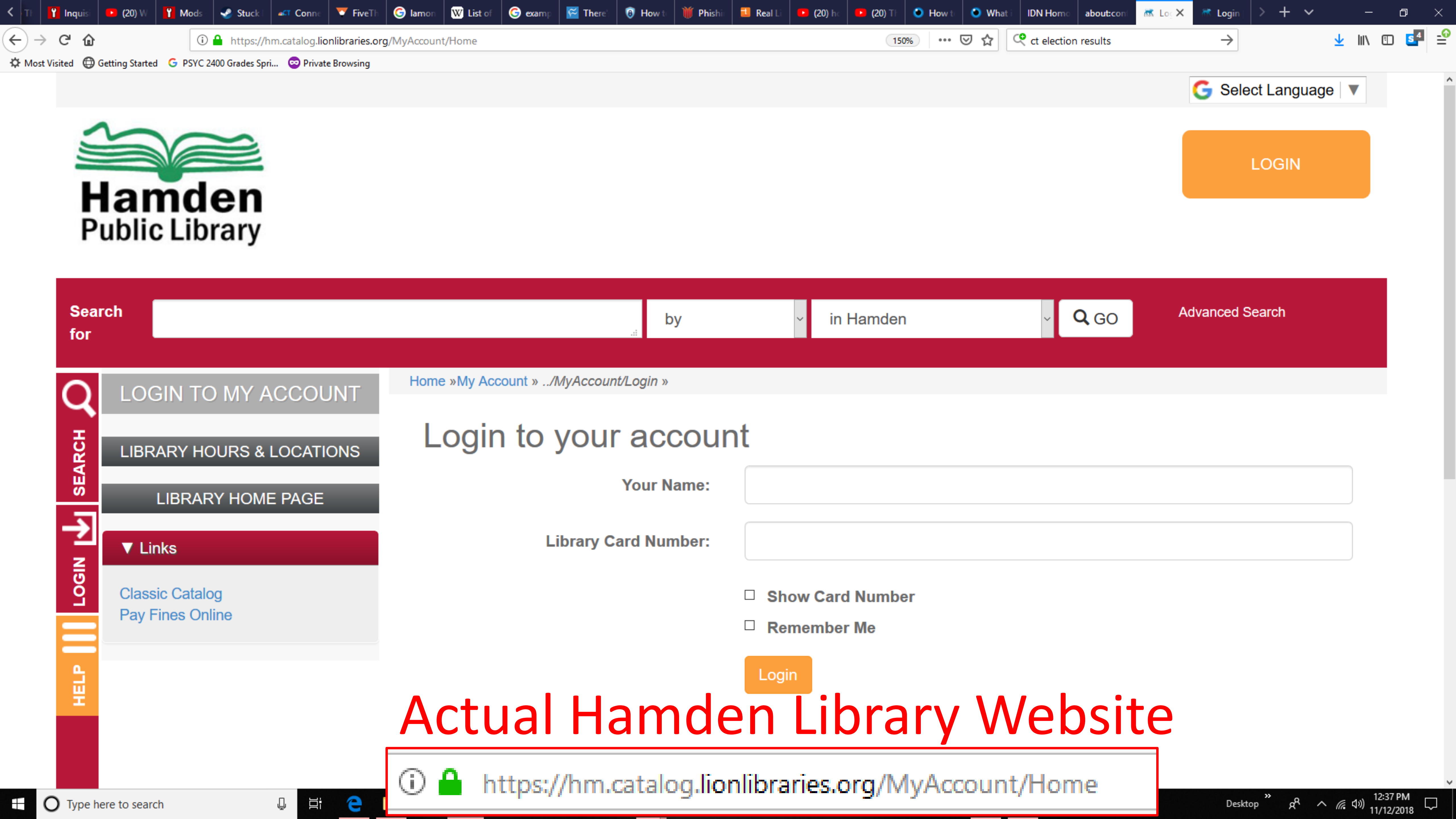
Library Card Number:

□ Show Card Number

□ Remember Me

Login

Fake Hamden Library Website



Home »My Account » ../MyAccount/Login »

Login to your account

Your Name:

Library Card Number:

□ Show Card Number

□ Remember Me

Login

Actual Hamden Library Website

https://hm.catalog.lionlibraries.org/MyAccount/Home

Phishing Pop-up Scams

Sometimes you will end up on a phishing website through no fault of your own even if you didn't click on anything.

The cause is malicious ads that contain a script that tell your browser to go to a phishing website

Usually these sites say that you won something or your device has a virus and want you to press a button to "fix now" or "claim your prize"

The popup may also disable your 'Back' or button through constant redirects and might not even let you close the window, it just says you can't leave until you click on the popup.

If you get stuck with a popup, either use the Task Manager to shut down the browser or reboot your device

This exploit is on the advertisers side, not your device, so Anti-Virus can't prevent it from happening (an ad blocker program might be able to) contact the website that you were viewing and let them know that some of the ads on their webpages are directing you to scam pages

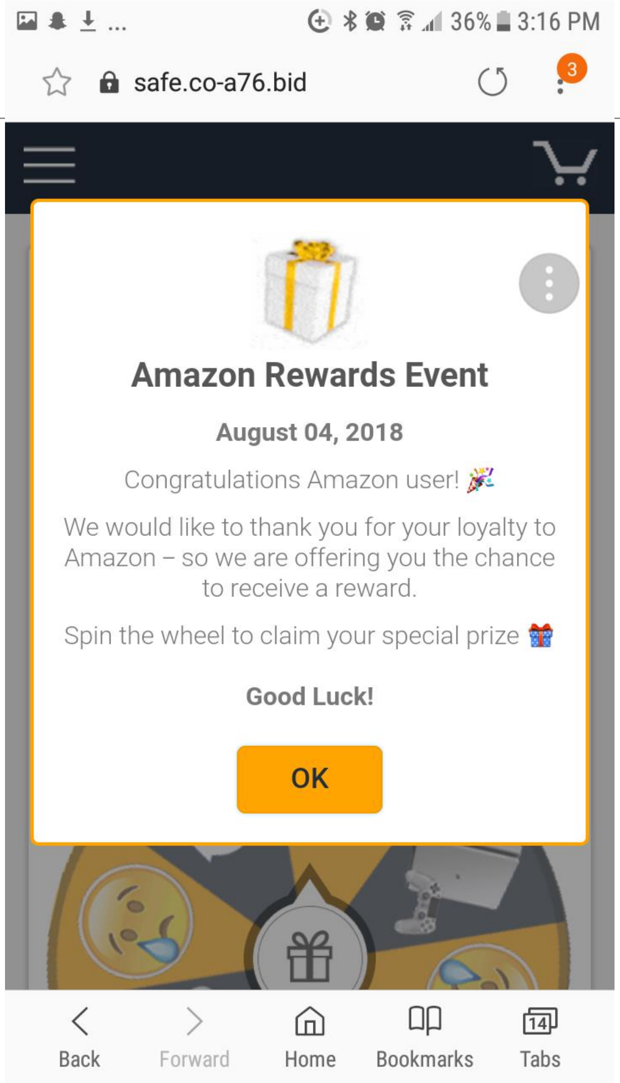
Phishing Popup Scams

Here are some examples of popups on an android phone.

These popups usually make the phone vibrate and try to make you click on their OK buttons without thinking.

Notice how they mimic the websites of the companies they are spoofing but their URL's are wrong (not Amazon or Google)

Never click on anything on these pages, try to use the back button or reboot the device if necessary



Amazon Rewards Event

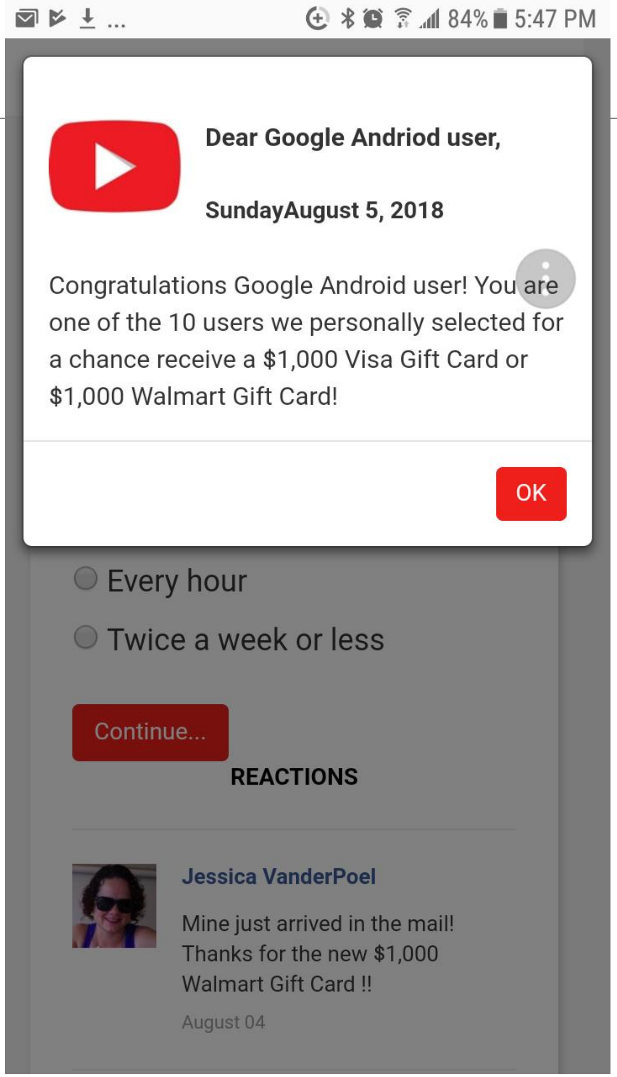
August 04, 2018

Congratulations Amazon user! 🎉

We would like to thank you for your loyalty to Amazon – so we are offering you the chance to receive a reward.

Spin the wheel to claim your special prize 🎁

Good Luck!



Dear Google Andriod user,

SundayAugust 5, 2018

Congratulations Google Android user! You are one of the 10 users we personally selected for a chance receive a $1,000 Visa Gift Card or $1,000 Walmart Gift Card!

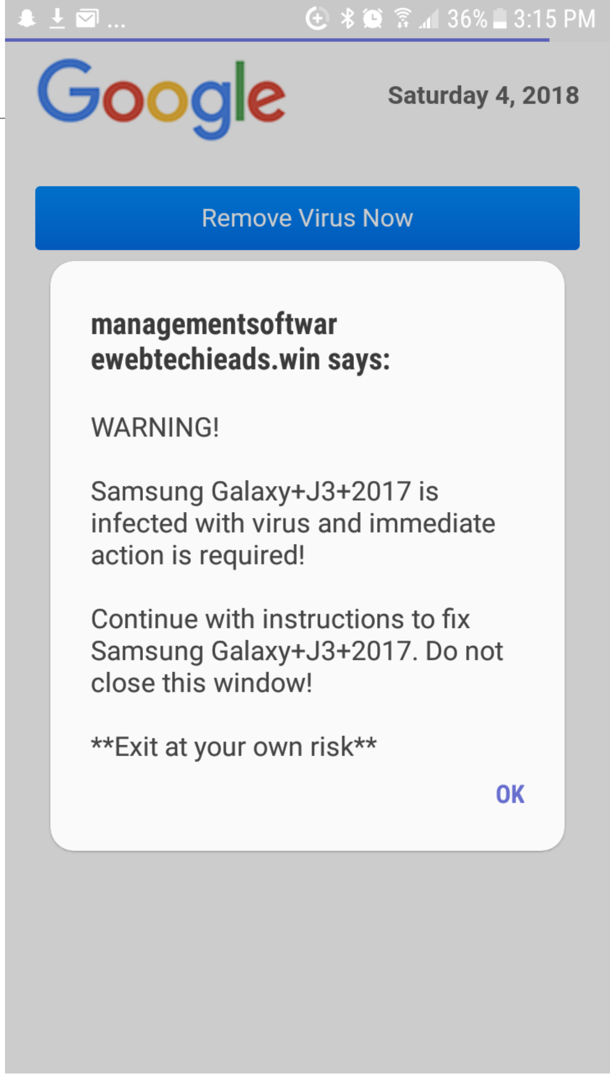
○ Every hour

○ Twice a week or less

Jessica VanderPoel

Mine just arrived in the mail! Thanks for the new $1,000 Walmart Gift Card !!

August 04



Saturday 4, 2018

managementsoftwarewebtechieads.win says:

WARNING!

Samsung Galaxy+J3+2017 is infected with virus and immediate action is required!

Continue with instructions to fix Samsung Galaxy+J3+2017. Do not close this window!

Exit at your own risk

Pop-up Scams on the PC

Much like mobile devices, browsers on personal computers are vulnerable to popups as well

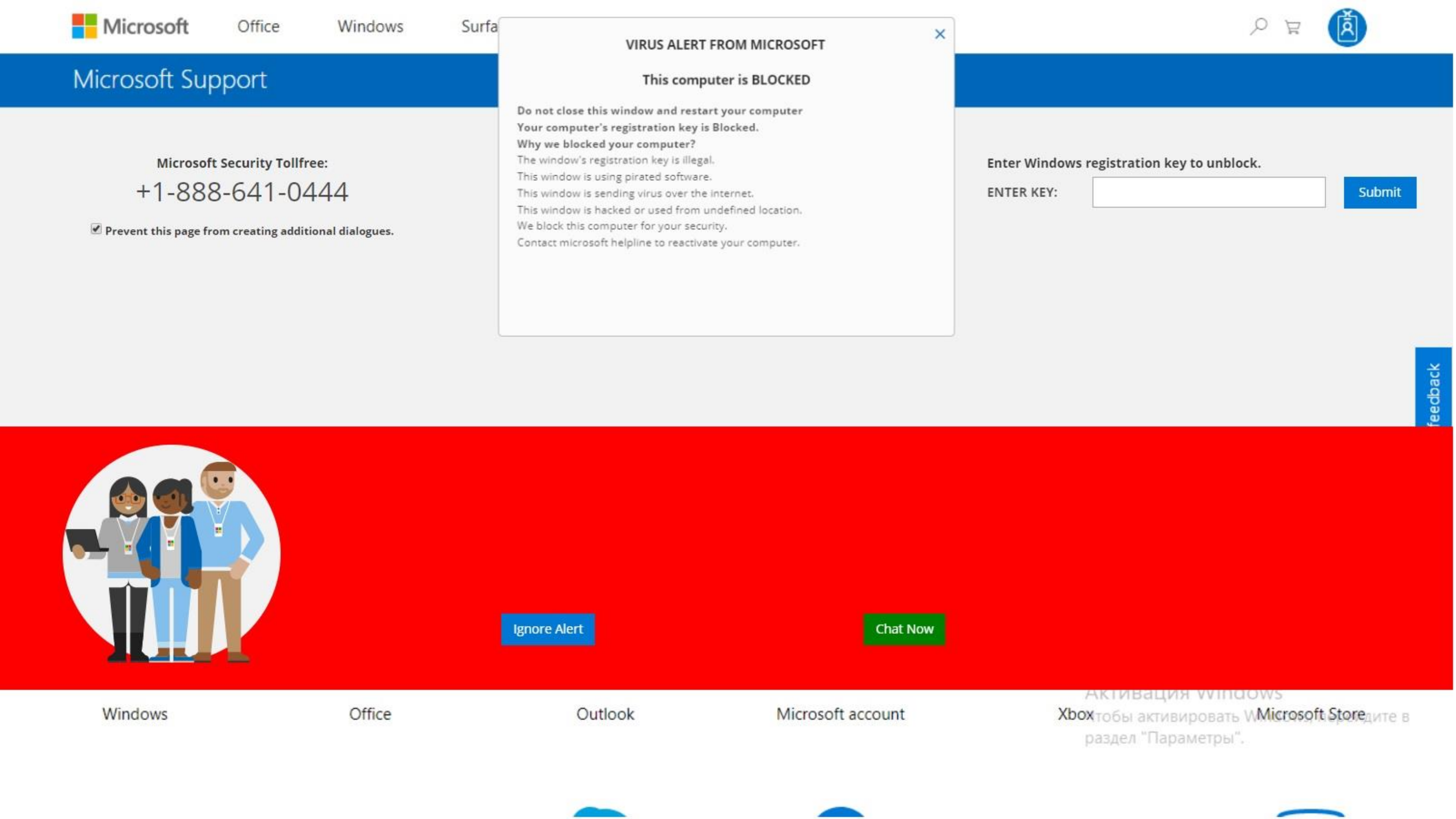
A popular scam is making the rounds now is one where attackers, pretending to be Microsoft, claim your computer is infected and that Microsoft has locked your computer until you provide the registration key.

The popup will not let you go back or exit out of the browser.

To get rid of it press **Control** & **Alt** & **Delete** then turn on task manager and shut down the browser. If that doesn't work restart your computer.

There are variations on this scam:

- Attackers claiming to be antivirus services that will help you get rid of the viruses on your computer. They will either do nothing and take payment or install actual malware on your device
- Attackers pretending to be government agencies accusing you of committing cybercrimes and demanding you "pay a fine" (usually with Bitcoin) or face prosecution.



VIRUS ALERT FROM MICROSOFT

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.
We block this computer for your security.
Contact microsoft helpline to reactivate your computer.

Microsoft Security Tollfree:

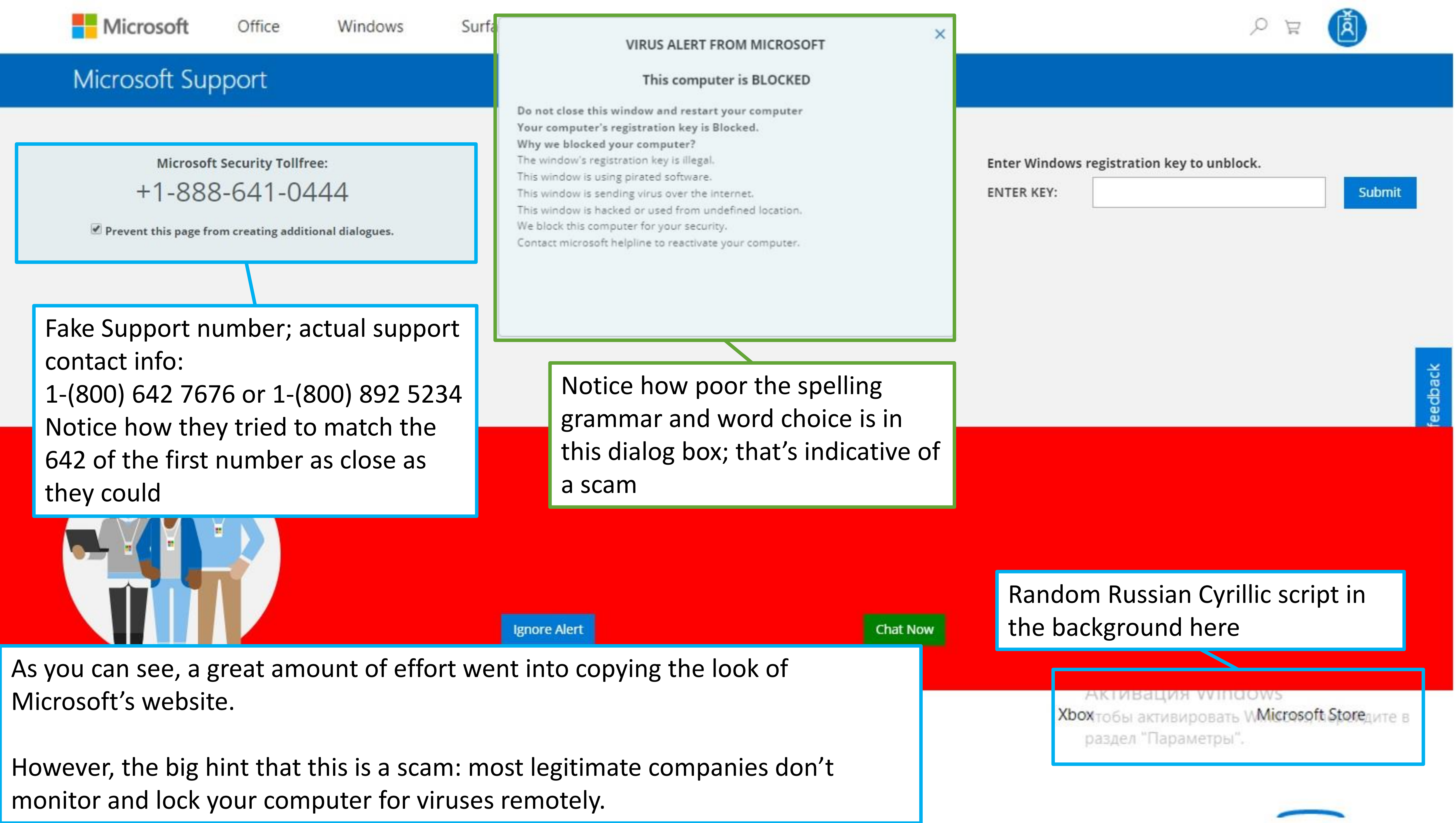
+1-888-641-0444

☑ **Prevent this page from creating additional dialogues.**

Enter Windows registration key to unblock.

ENTER KEY: ▭ Submit

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".



Microsoft Security Tollfree:

+1-888-641-0444

☑ Prevent this page from creating additional dialogues.

VIRUS ALERT FROM MICROSOFT ×

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.
We block this computer for your security.
Contact microsoft helpline to reactivate your computer.

Enter Windows registration key to unblock.

ENTER KEY: ________ Submit

Активация Windows
тобы активировать W ите в
раздел "Параметры".

Fake Support number; actual support contact info:
1-(800) 642 7676 or 1-(800) 892 5234
Notice how they tried to match the 642 of the first number as close as they could

Notice how poor the spelling grammar and word choice is in this dialog box; that's indicative of a scam

Random Russian Cyrillic script in the background here

As you can see, a great amount of effort went into copying the look of Microsoft's website.

However, the big hint that this is a scam: most legitimate companies don't monitor and lock your computer for viruses remotely.

Microsoft Support Scam

Hints that it is a scam

1. Misspellings in the instructions and text on the page
2. The Russian lettering in the bottom right of the screen
3. Reputable companies/Government agencies don’t use popups to lock out your computer then demand information on the same screen to unblock it
4. There is a fake tech support number in the top left, actual support contact info:
   1-(800) 642 7676 or 1-(800) 892 5234
   Notice how they tried to match the 642 of the first number as close as they could

The fake support number is why you should never trust the support contact info on these popup pages, you will most likely get connected with the attackers who will lie to you.

Countermeasures

Always be vigilant of unsolicited emails, especially ones that require immediate action

If the email's author is known to you, try to contact them by other means before clicking on the link or downloading the attachment

If the email says there is a problem with your account, go to the website yourself and log in there, if there is a problem the account should say so.

Be suspicious when browsing the web, remember that you are a target

Report Phishing attempts to your email provider, the organization that was impersonated and the U.S. Government

Utilize different email addresses for different purposes

Enable Two-Factor Authentication wherever possible

Backup all your important data in an external hard drive/cloud storage system

Updates your operating system/browser/anti-virus programs regularly

Reporting Phishing Attempts

To your email provider:

- Most email providers have a button that allows you to report a message as a phishing attempt
- If not you can always forward the email to their customer support team

To the organization that is being impersonated:

- In this case just contact their customer service team by phone or email
- Generally forwarding the phishing message is a good idea as it lets them see what you received

To the government:

- Both the US-CERT Anti-Phishing Working Group (AFWG) and the Federal Trade Commission accept reports on phishing emails
- Report phishing to the US-CERT APWG at phishing-report@us-cert.gov & reportphishing@apwg.org
- Report phishing (and spam) to the FTC at spam@uce.gov & https://www.ftc.gov/complaint
- If you are the victim of a phishing attack https://www.identitytheft.gov/ allows you to report it and get information on next steps

Additional Resources

https://www.kent.edu/sites/default/files/file/DontGetHooked_Poster_0.jpg

https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

https://www.webopedia.com/TERM/P/phishing.html

https://www.theatlantic.com/technology/archive/2018/09/phishing-is-the-internets-most-successful-con/569920/

https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

https://www.consumer.ftc.gov/articles/0003-phishing

https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams

https://www.sans.org/security-awareness-training/

https://www.avg.com/en/signal/what-is-phishing

https://www.consumer.ftc.gov/articles/0350-text-message-spam

Additional Resources

https://www.consumer.ftc.gov/articles/0038-spam

https://www.consumer.ftc.gov/articles/0009-computer-security

https://www.computerhope.com/jargon/u/url.htm

https://www.youtube.com/watch?v=KMml5NoY4iI How to clone a website

https://www.lifewire.com/definition-of-uniform-resource-locator-817778

https://computer.howstuffworks.com/internet/basics/internet-infrastructure7.htm

https://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html

https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/

https://privacy.net/dns-spoofing/