

Phishing Links – Fighting the Good Fight

Presented by Jason Tolley
Sr. Network Administrator
Wisconsin Reinsurance Corporation
jtolley@thewrcgroup.com
877-280-3124

<https://bit.ly/2QhW4vc>



Agenda

- Introduction
- Why are we here and why this is important (What's the big deal)
- Threat overview – Phishing
- Red Flag Emails
- Anatomy of a URL
- Understanding URLs
- Common URL Phishing Tricks
- Recap

Who is this guy?

- Sr. Network Administrator
 - 19+ years with WRC
 - Responsible for the technical management and support of the backend infrastructure
 - 10+ years additional focus on Information Security – Securing WRC's computing infrastructure and data assets

Why are we here?

Why are we here?

Recognize - that there are people out there that want to take advantage of us for their personal gain or desire to just wreak havoc.

Responsibility – Feeling that you need to do your part for your organization to protect the company and the clients you serve.

Information – Learn something new or reinforce what you may already know.

Connection – Unexplained or uncontrollable desire to get in touch with your inner nerd OR more likely to come together with your peers to compare notes and share experiences.

The reality is phishing attacks are a constant threat to businesses (as well as personally). They are not going anywhere because they are still effective. As time goes on phishing attacks are evolving and are becoming increasingly sophisticated.



What's the big deal

Successful Phishing attacks can:

- Put personal information at risk
- Cause financial loss for victims
- Put business data and systems at risk
- Damage your company's reputation
- Put you out of business

Threat Overview – Phishing

- **Estimated that 3.7 billion people send around 269 billion emails every single day. Researchers suggest that almost one in every 2,000 of these emails is a phishing email, which means around 135 million phishing attacks are attempted every day.**
- **Nearly 86% of all phishing attacks target U.S. entities**
- **86% of Email Attacks are “Malwareless”**
- **URL phishing detections increased 269% in 2019**
- **One-third of all data breaches in 2019 involved phishing**
- **48% of malicious email attachments are Microsoft Office Files**
- **84% of SMBs targeted by phishing attacks**
- **74% of All Phishing Websites Use HTTPS Protocol**
- **Cyber criminals are creating an average of around 1.4 million phishing websites every month**



Red Flag Emails

Things that should make you go hmmmm...

1. Emails Insisting on Urgent Action

- Fluster or distract the target.
- Threatens a negative consequence if the action is not taken

2. Emails Containing Spelling Mistakes

- professional email sources that contains spelling mistakes or grammatical errors should be treated with suspicion.

3. Emails with an Unfamiliar Greeting

- Those addressed to “Dear XXXXX” when that greeting is not normally used,
- Contains language not often used by friends or co-workers.

Red Flag Emails

Things that should make you go hmmm...the sequel

4. Inconsistencies in Email Addresses

- Random checking of senders' email addresses.
- Checking the sender email address against previous emails received from the same person.

5. Inconsistencies in Links and Domain Names

- Malicious websites can easily be disguised as genuine links.
- Hover a mouse pointer over a link in an email.

6. Be Wary of Suspicious Attachments

- File attachments should be treated suspiciously.
- Unexpected file attachments should raise suspicion even more
- Unfamiliar extension (.vbs, .exe, .ps1 .bat, etc.).

Red Flag Emails

Things that should make you go hmmmm...the final chapter

7. Emails That Seem Too Good to Be True

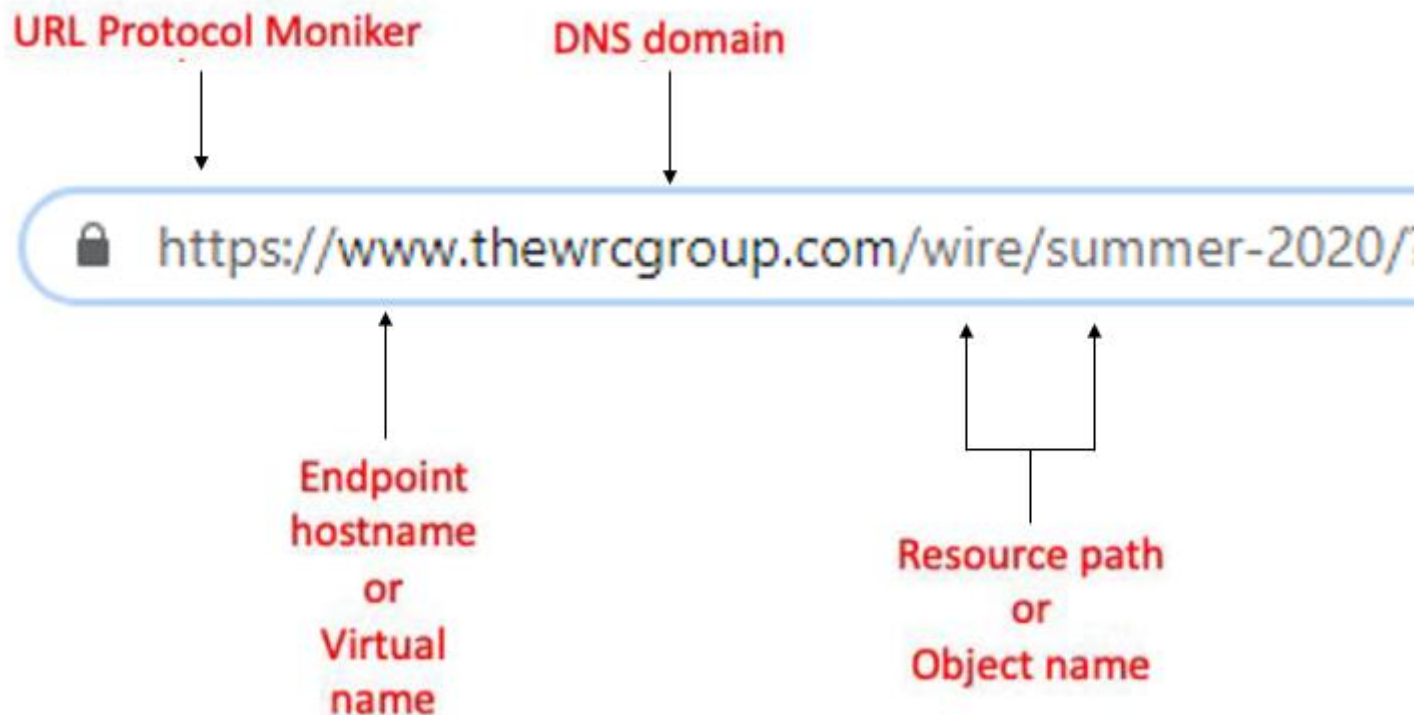
- Promise that they will benefit by clicking.
- Appeal to the target's curiosity or greed.
- The intended targets have not usually initiated contact.

8. Emails Requesting Login Credentials, Payment Information or Other Sensitive Information

- No one reputable will EVER ask for this kind of information.



Anatomy of a URL



Understanding URLs

Basics

DNS domain name

- Starts after the first period after the hostname
- End before the first single slash

🌐 `https://www{example.com}/subpath/subpath/resourcename`

🌐 `https://www{SubDomainunderMainDomain.example.com}/subpath/subpath/resourcename`

Understanding URLs

Basics

DNS Top-Level Domain (TLD) name

- Starts after the last period and before the first slash
- Ends before the first slash

 `https://www.example{com}/subpath/subpath/resourceName`


- Examples: .com .net .org .gov .mil .biz
- There are over 1000 TLD names
 - <https://www.iana.org/domains/root/db>


Understanding URLs

Basics

Variables

- Anything after the first “?” is a variable being passed back to the host to be evaluated.
- Often used to track users



 <https://www.example.com/s3/1234567/my-survey?variable=value>

Can be crafted to obtain sensitive data:

- Usernames
- Passwords
- Session tokens

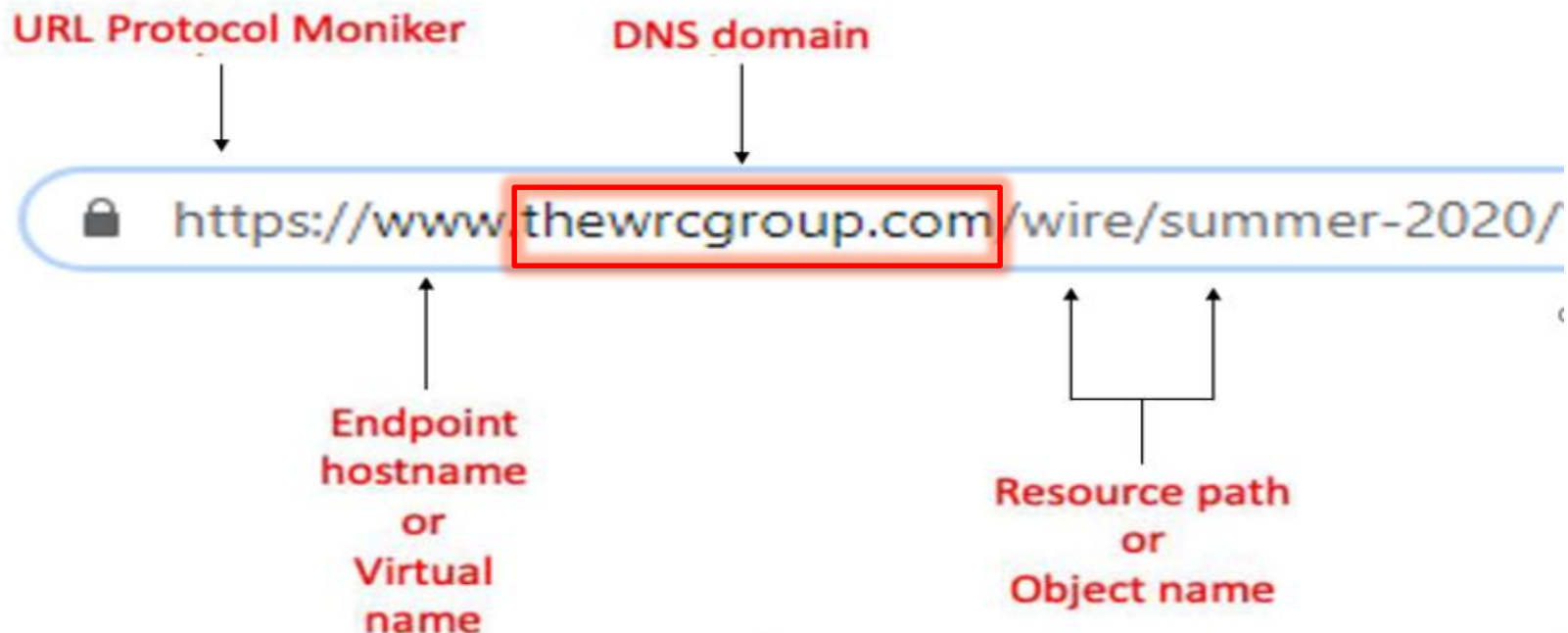
Information can be pulled from:

- Shared Systems
- Browser History
- Browser Cache

Understanding URLs

Basics

- The most important URL analysis skill you can know or teach is figuring out what the TRUE DNS domain is!



Understanding URLs

Basics

- There is a BIG difference between.....

DNS domain

⌚ {example.com.domain.com}

DNS domain

⌚ {example.com}/domain.com

DNS domain

🔍 {example.com.domain}/com

Common URL Phishing Tricks

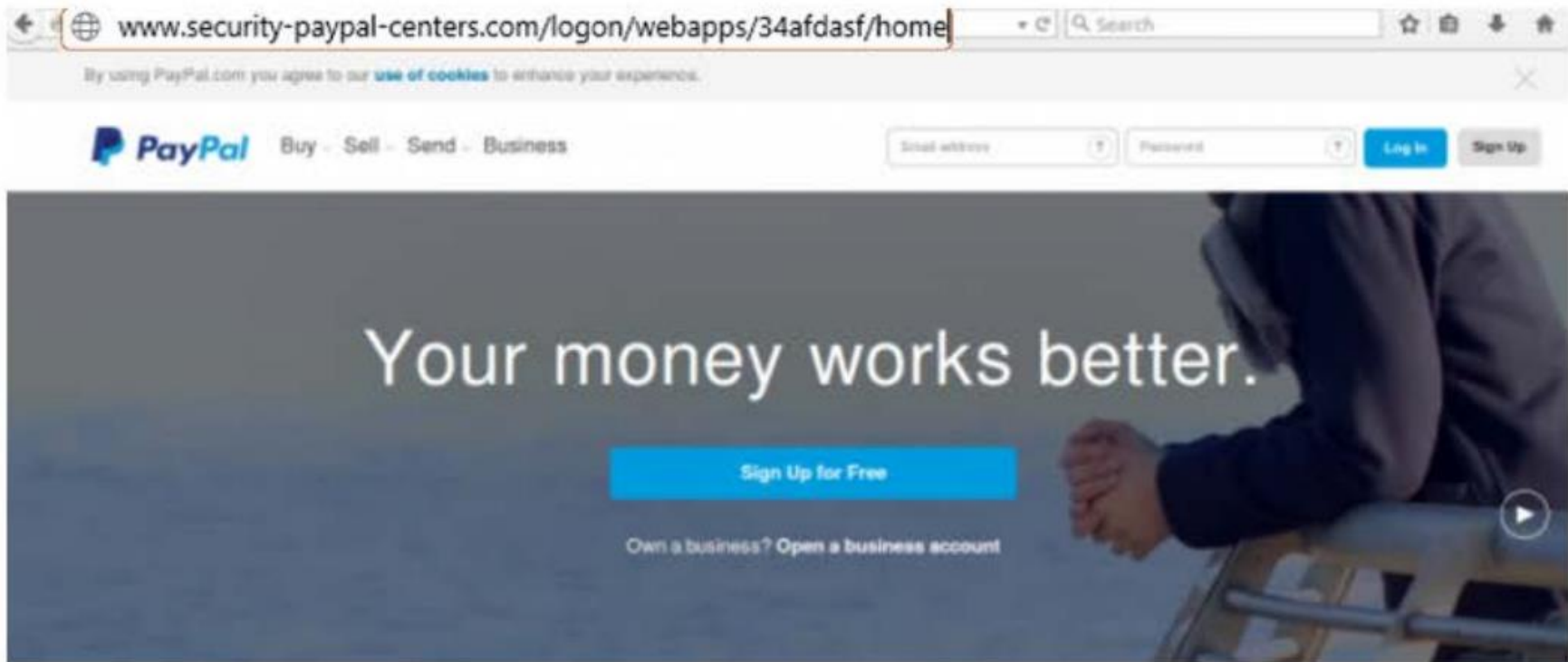
**Spotting malicious URLs – Look-Alike Domains
Subdomain tricks**

 [www.paypal.com.bank/logon?user=\[REDACTED\]@gmail.com](http://www.paypal.com.bank/logon?user=[REDACTED]@gmail.com)

**The Domain is:
paypal.com.bank
NOT
paypal.com**

Common URL Phishing Tricks

Spotting malicious URLs – Look-Alike Domains
Domain tricks



The Domain is:
security-paypal-centers.com
NOT
paypal.com

Common URL Phishing Tricks

Complaint Filed: jsmith



Peg Mickleson <pmickleson@docsendportal.com>

John Smith

Thursday, February 28, 2019 at 1:13 PM

[Show Details](#)

John Smith,

Peg Mickleson Has Sent You a Notice: "Code of Conduct Violation 201902-jsmith" to Sign

Peg Mickleson (WRC) says:

"Please review and sign Notice: Code of Conduct Violation-201902-jsmith"

Click here to review and sign **Notice: Code of Conduct Violation-201902-jsmith**.

<https://wrcdocs.docsendportal.com/notices?rid=9IQrgSd>

Log in using your email address and password.

After you sign **Notice: Code of Conduct Violation-201902-jsmith**, all parties will receive a final PDF copy by email.

This message was sent to you by "Peg Mickleson" who is using the DocSendPortal Encrypted File Sending Service. If you would rather not receive email from this sender you may contact the sender with your request. Copyright DocSendPortal 2019 All rights reserved.

Log In



Please log in to your account

Email address

Password

LOGIN

[No account? Sign up for free](#)

Common URL Phishing Tricks

Outlook Update - Action Required

Derek Lipp [dlipp@thewrcgroup.com]

To: [redacted]

Thursday, February 08, 2018 12:36 PM

Just a heads up, there have been some updates to our mail server to enable new features. Please follow the instructions below by the end of business today. Thanks!

Scheduled Maintenance

What: Outlook Maintenance

Who: All Personnel

Date: 02/08/2018-02/10/2018

Time: 7:00 a.m - ongoing

Impact: Upgrades are occurring for Outlook 2016 integration. This will allow for better synchronization of contacts and calendars. All users are required to go through the integration process.

Visit [https://owa.thewicgroup.com/owa/auth/logon.aspx?id=\[redacted\]](https://owa.thewicgroup.com/owa/auth/logon.aspx?id=[redacted]) to go through the integration process for your account.

Please finish this process by the end of the day.

Derek Lipp | Systems Administrator

Wisconsin Reinsurance Corporation

Direct: (608) 441-3147 | Toll Free: (877) 280-3147 | Fax: (608) 441-3100

dlipp@thewrcgroup.com | thewrcgroup.com

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

○ Valid, Trusted Email Message:

- In Outlook, From displays:
- Derek Lipp

○ Invalid, Un-trusted Email Message:

- In Outlook, From displays:
- Derek Lipp
[dlipp@thewrcgroup.com]

Common URL Phishing Tricks

URL Shortening

- URL shortening services covert longer URLs into “shortcut URLs”
 - Bit.ly, goo.gl, t.co, tinyurl.com
- Initially intended to just help people type them in more easily or save space on Twitter (140 character limit)
- Very often used maliciously to hide intent or redirection

https://www.google.com/search?gs_ssp=eJzj4tTP1Tcwyk4zMjFg9BJOLC0uKUrMyUzMUyjOSC3ISC1KAQCe1wqt&q=australian+shepherd&rlz=1C1CHBD_enUS810US810&oq=australian+sh&aqs=chrome.1.0j46j69i57j0l2j46j0l2.12429j0j4&sourceid=chrome&ie=UTF-8

<https://bit.ly/31yTreX>



australian shepherd puppy



Settings

Tools

About 89,800,000 results (0.69 seconds)

www.akc.org › Dog Breeds ▾

Australian Shepherd Dog Breed Information

Aug 4, 2020 - The **Australian Shepherd** is an intelligent working dog of strong herding and guarding instincts. He is a loyal companion and has the stamina to work all day. He is well balanced, slightly longer than tall, of medium size and bone, with coloring that offers variety and individuality.

People also ask



Australian Shepherd



Dog breed

Convert

- Convert short URLs to “exploded” URLs
- Example: <https://www.expandurl.net/expand>

<https://bit.ly/2QhW4vc>

RESULTS FOR [HTTPS://BIT.LY/2QHW4VC](https://bit.ly/2QhW4vc)



Title: WRC | Reinsurance Solutions & Resources | Comprehensive Reinsurance

Short URL: <https://bit.ly/2QhW4vc>

Redirects: 2 ([hide details](#))
1. <http://www.thewrcgroup.com/>
2. <https://www.thewrcgroup.com/>

Long URL: <https://www.thewrcgroup.com/>

EXTRA INFORMATION

Meta Description: With over 85 years of experience in creating customized reinsurance solutions, WRC provides industry-leading reinsurance products & services. Our customized reinsurance contracts are carefully designed to meet the unique needs of each mutual partner, providing peace of mind, operational support & financial protection.

Meta Keywords: *No Keywords*

Content-Type: text/html; charset=UTF-8

Canonical URL: <https://www.thewrcgroup.com/>

Google Safe Browsing: OK - This link appears to be safe!
[Advisory provided by Google.](#)

Common URL Phishing Tricks

URL Encoding

URLs can be represented using IP addresses and special characters to camouflage the real domain name.

Example:

IP address: <https://35.192.90.70>
www.thewrcgroup.com

Special characters:

<https://%77%77%77.%54%48%45%77%52%43%47%52%4F%55%50.%63%6F%6D>
www.thewrcgroup.com

Common URL Phishing Tricks

Overly Long URLs

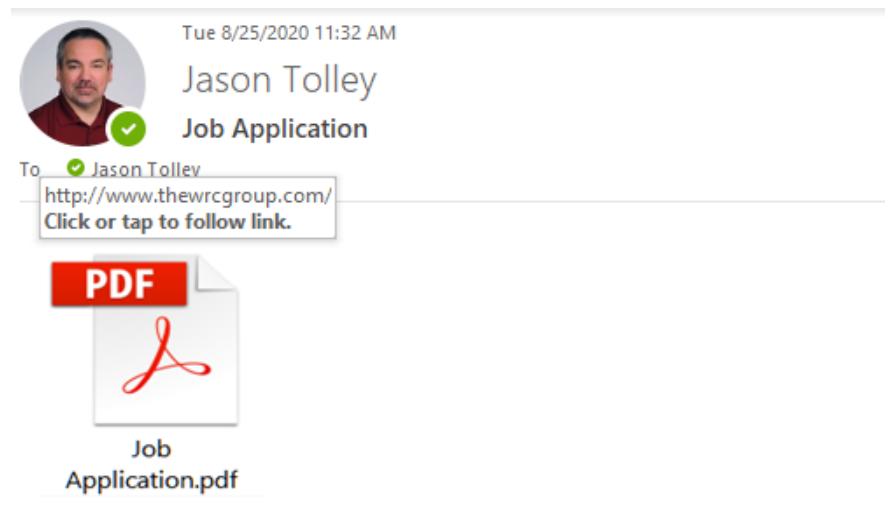
Phishers use overly long URLs to make it more difficult for the user hovering over the link to see it or even want to see it all.

Ex: <https://innocentwebsite.com/irs.gov/logon/fasfjdsafalj-divafasfasdfdvjeffafsfawqeavpompfiif5asmfasfpeagasasdpjsafasfasdfiawfasfsadfspadf asfsadfasdvasdfasdfsdljiottbpoaovmas6sppaasd gatapapdgaadatkaoapjwkgjapbabaoe eadafdafddaasff/afasdfaetpriadagasdg1fagagasddsafdsfdsafdsaadfacsvjsdavjastkjei igaadagadgetimppbhesstdfasdaetladasvaass1dafadfkfj89sadfajsgagapomfieeeirmagab aetesragaddlapddlteya'/jpafdasfpoifuafdterqpbfghfdghfad/ght.php>

Common URL Phishing Tricks

File Attachments

- File attachment is actually a wolf in sheep's clothing
 - Not actually the type of file it is displaying
 - Actually points to a URL link





Jason Tolley | Senior Network Administrator

Wisconsin Reinsurance Corporation

Direct: (608) 441-3124 | Toll Free: (877) 280-3124 | Fax: (608) 441-3101

Common URL Phishing Tricks

→  portal.thewrcgroup.com/

 **Certificate Information**

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: portal.thewrcgroup.com

Issued by: Thawte RSA CA 2018

Valid from 4/28/2020 **to** 6/13/2022

Top trusted Certificate Authorities:

- Digicert/Thawte
- RapidSSL
- Symantec
- GeoTrust

Questionable Certificate Authorities:

- Google “free SSL”
- Legitimate services
- Abused by bad actors

Digital Certificates

- Just because it has the lock does not mean that the site is not malicious
 - Does not mean you can automatically trust the site
- More and more phishing websites have valid “Trusted” certificates
- This is because of some “Certificate Authorities” do minimal validation

Remember

Opening URLs or File Attachments

Doing so can lead to:

- Immediate exploitation (remote control, malware, ransomware, data exfiltration, etc.)
- Sending computer or network information:
 - IP address, Operating System information, Web Browser information, Location, etc.
- Sending your password hash to the remote attacker

What can I do?

Personal Defenses

- Educate yourself and your co-workers (www.knowbe4.com)
- Always hover before you click
- Don't download or open unexpected files
- Investigate or ignore suspicious URLs (www.brightcloud.com)
- Submit to a malware inspection service (www.virustotal.com)
- Stay patched
- Make sure you are running Anti-malware software and keep it up-to-date
- Remember the Red Flags and live by them

What can I do?

It's ok to hover

- Always, Always, Always “hover” over ALL URLs first to reveal them
- What you see in the “display” URL may not be the true destination URL



Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions ~~without interruption~~.

Please sign in to your account at <https://www.bankofamerica.com>

to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

<http://bit.do/ghsdfhgdsd>

What can I do"

Investigate or ignore suspicious URLs

<https://www.brightcloud.com/tools/url-ip-lookup.php>

Look up URL or IP:

☐

I'm not a robot



LOOK UP

If you have a mutually executed agreement with Webroot, those terms apply to your use of the BrightCloud Service. If you do not have a mutually executed agreement with Webroot, by clicking "LOOK UP", you agree to the terms and conditions of the BrightCloud Threat Intelligence Service for Enterprise Agreement.

Request a Change:

URL or IP: *

Optional: [I would like to suggest a category for this URL](#)

Your email: *



WWW.THEWRCGROUP.COM

Web Reputation:



- Trustworthy (100 of 100)

[Request a reputation change](#)

Web Category:

- Financial Services

[Request a category change](#)

Web Reputation Influences:

- No infections past 12 months
- High popularity
- 142 months old (established)

Impact:



What can I do?

Submit to a service:

<https://www.virustotal.com/gui/home/url>
(70+ different anti-virus engines)

0
/ 64

Community
Score

✓ No engines detected this URL

<http://www.thewrcgroup.com/>
www.thewrcgroup.com

DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	✓ Clean	AegisLab WebGuard ✓ Clean
AlienVault	✓ Clean	Antiy-AVL ✓ Clean
Avira (no cloud)	✓ Clean	Baidu-International ✓ Clean
BitDefender	✓ Clean	Blueliv ✓ Clean
C-SIRT	✓ Clean	Certly ✓ Clean
CLEAN MX	✓ Clean	Comodo Site Inspector ✓ Clean
CyberCrime	✓ Clean	desenmascara.me ✓ Clean
Dr.Web	✓ Clean	Emsisoft ✓ Clean
ESET	✓ Clean	Fortinet ✓ Clean
FraudScore	✓ Clean	FraudSense ✓ Clean
G-Data	✓ Clean	Google Safebrowsing ✓ Clean
K7AntiVirus	✓ Clean	Kaspersky ✓ Clean

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



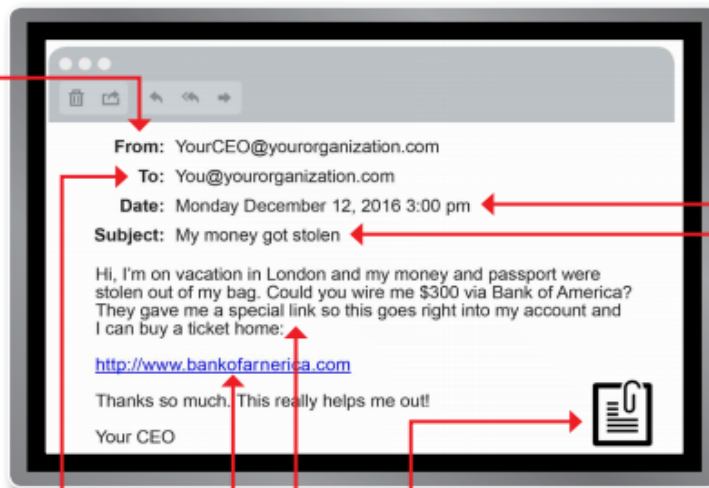
TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?


THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users into visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Alike Domains


Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings


 Microsoftonline
<v5pz@onmicrosoft.com>

 www.llnkedin.com

Brand name in URL, but not real brand domain

 ee.microsoft.co.login-update-dec20.info


 www.paypal.com.bank/logon?user=johnsmith@gmail.com

 ww17.googlechromeupdates.com/


Brand name in email address but doesn't match brand domain

 Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

 devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

 <https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D>

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

 <https://bit.ly/2SnA7Nm>

Domain Mismatches

 Human Services .gov
<Despina.Orrantia6731610@gmx.com>

 <https://www.le-blog-qui-assure.com/>

Strange Originating Domains

 MAERSK
<info@onlinealxex.com.pl>


Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

 <http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndfjnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdgfgjhfgd/ght.php>

File Attachment is an Image/Link


It looks like a file attachment, but is really an **image file with a malicious URL**.

 INV39391.pdf
52 KB

<https://d.pr/free/f/jsaoc>
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

 t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

THANK YOU!

- Attendees
- WRC Reinsurance Team
- Information Services Team
- Technical editing assistant
“Gilbert”

