

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-Like Domains

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

Slight Misspellings

 Microsoftonline
<v5pz@onmicrosoft.com>

 www.lInkedin.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/2SnA7Fnm>

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-sajdkjndfjnbkasldjfbkajsdjfbkjbasdf/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