UNDERSTANDING PHISHING

INKY

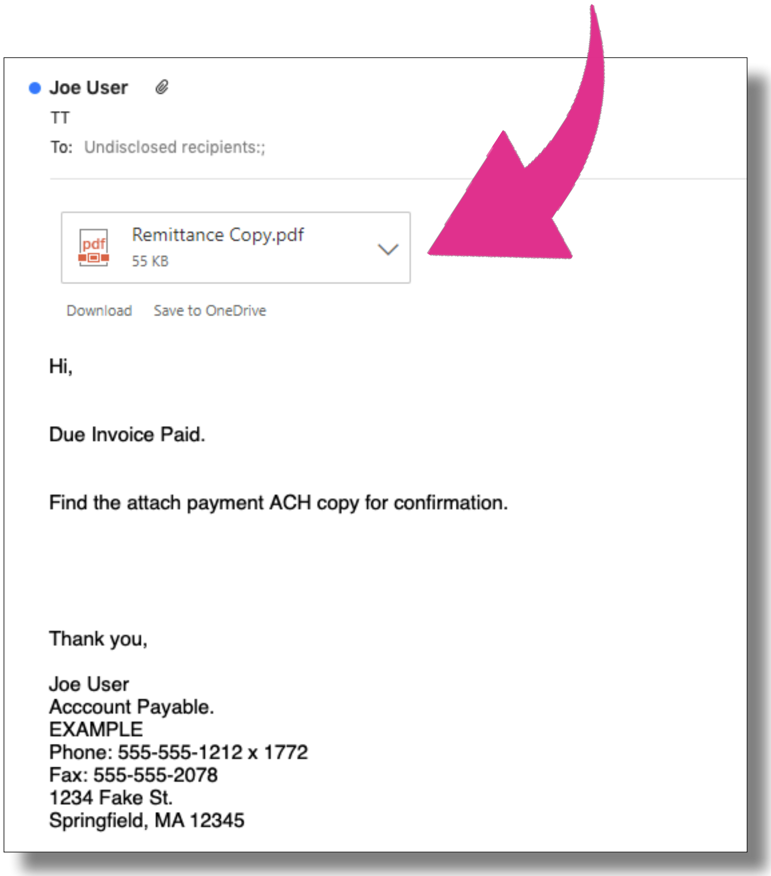
Fake Attachments

Scammers have been sending malicious attachments for decades. These files are delivered in an email that does something bad when opened. We'll unwrap how these emails are still outsmarting traditional email filters and getting through to end-users

What are Fake Attachments?

Scammers have been sending malicious attachments for decades. These are files delivered alongside an email that do something bad when opened, and most mail protection systems have multiple countermeasures against them. Recently, however, we've seen a new trend: *malicious fake attachments.*

A fake attachment is an image embedded in an email that looks like the attached file icon used in a common mail client like Microsoft Outlook.



Joe User
TT
To: Undisclosed recipients:;

Remittance Copy.pdf
55 KB

Hi,

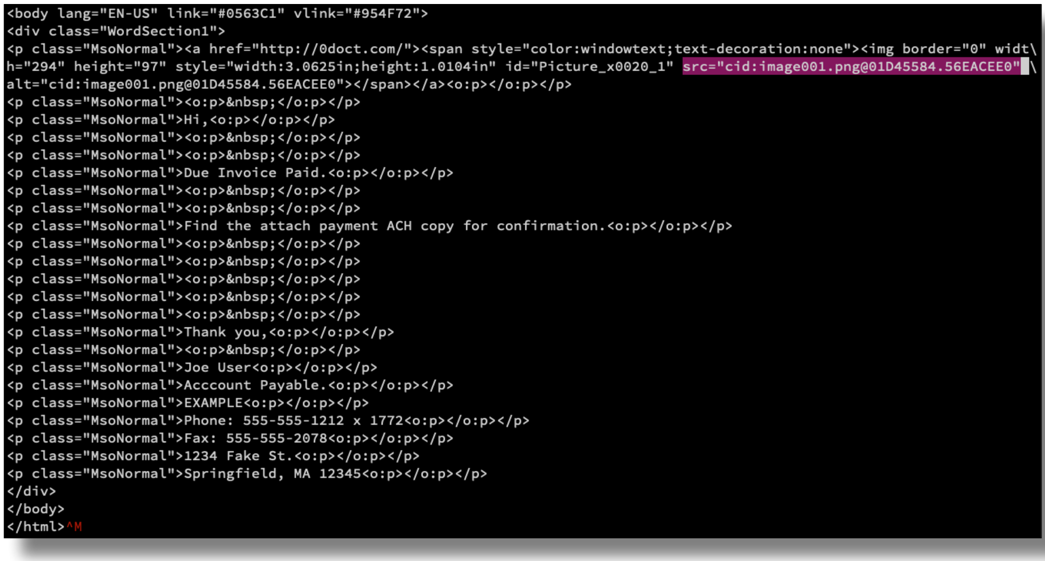
Due Invoice Paid.

Find the attach payment ACH copy for confirmation.

Thank you,

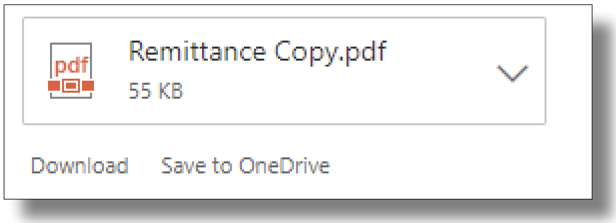
Joe User
Acccount Payable.
EXAMPLE
Phone: 555-555-1212 x 1772
Fax: 555-555-2078
1234 Fake St.
Springfield, MA 12345

The screen shot above is of a real email that INKY blocked for a customer. (We have replaced all the identifying information but it's otherwise identical to what INKY analyzed.) Notice the attachment labeled *Remittance Copy.pdf*? Let's look under the hood at the HTML of this email to see what that really is:

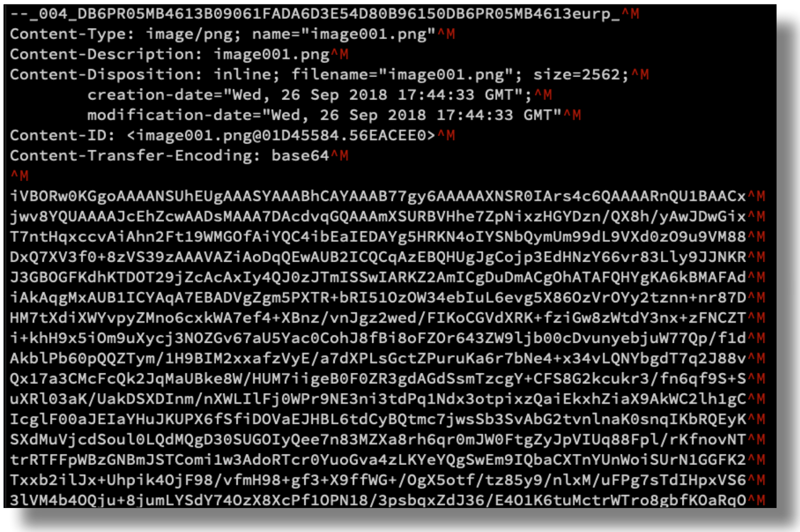


```
<body lang="EN-US" link="#0563C1" vlink="#954F72">
<div class="WordSection1">
<p class="MsoNormal"><a href="http://0doct.com/"><span style="color:windowtext;text-decoration:none"><img border="0" widt\
h="294" height="97" style="width:3.0625in;height:1.0104in" id="Picture_x0020_1" src="cid:image001.png@01D45584.56EACEE0" \
alt="cid:image001.png@01D45584.56EACEE0"></span></a><o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal">Hi,<o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal">Due Invoice Paid.<o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal">Find the attach payment ACH copy for confirmation.<o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal">Thank you,<o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<p class="MsoNormal">Joe User<o:p></o:p></p>
<p class="MsoNormal">Acccount Payable.<o:p></o:p></p>
<p class="MsoNormal">EXAMPLE<o:p></o:p></p>
<p class="MsoNormal">Phone: 555-555-1212 x 1772<o:p></o:p></p>
<p class="MsoNormal">Fax: 555-555-2078<o:p></o:p></p>
<p class="MsoNormal">1234 Fake St.<o:p></o:p></p>
<p class="MsoNormal">Springfield, MA 12345<o:p></o:p></p>
</div>
</body>
</html>^M
```

The portion highlighted in purple gives the URL source of an image tag. The referenced image looks like this:



You'll notice something strange about the URL too: most images URLs start with http: or https: whereas this one starts with cid:. This is because it is uses the *Content-Id* URL scheme, a way for HTML in an email to reference data *attached to the email itself*. You can see below what exactly this cid: URL references (excerpted):



```
--_004_DB6PR05MB4613B09061FADA6D3E54D80B96150DB6PR05MB4613eurp_^M
Content-Type: image/png; name="image001.png"^M
Content-Description: image001.png^M
Content-Disposition: inline; filename="image001.png"; size=2562;^M
        creation-date="Wed, 26 Sep 2018 17:44:33 GMT";^M
        modification-date="Wed, 26 Sep 2018 17:44:33 GMT"^M
Content-ID: <image001.png@01D45584.56EACEE0>^M
Content-Transfer-Encoding: base64^M
^M
iVBORw0KGgoAAAANSUhEUgAAASYAAABhCAYAAAB77gy6AAAAAXNSR0IArs4c6QAAAARnQU1BAACx^M
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAmXSURBVHhe7ZpNixzHGYDzn/QX8h/yAwJDwGix^M
T7ntHqxccvAiAhn2Ft19WMGOfAiYQC4ibEaIEDAYg5HRKN4oIYSNbQymUm99dL9VXd0zO9u9VM88^M
DxQ7XV3f0+8zVS39zAAAVAZiAoDqQEwAUB2ICQCqAzEBQHUgJgCojp3EdHNzY66vr83Lly9JJNKR^M
J3GBOGFKdhKTDOT29jZcAcAxIy4QJ0zJTmISSwIARKZ2AmICgDuDmACgOhATAFQHYgKA6kBMAFAd^M
iAkAqgMxAUB1ICYAqA7EBADVgZgm5PXTR+bRI51OzOW34ebIuL6evg5X86OzVrOYy2tznn+nr87D^M
HM7tXdiXWYvpyZMno6cxkWA7ef4+XBnz/vnJgz2wed/FIKoCGVdXRK+fziGw8zWtdY3nx+zFNCZT^M
i+khH9x5iOm9uXycj3NOZGv67aU5Yac0CohJ8fBi8oFZOr643ZW9ljb00cDvunyebjuW77Qp/f1d^M
AkblPb60pQQZTym/1H9BIM2xxafzVyE/a7dXPLsGctZPuruKa6r7bNe4+x34vLQNYbgdT7q2J88v^M
Qx17a3CMcFcQk2JqMaUBke8W/HUM7iigeB0F0ZR3gdAGdSsmTzcgY+CFS8G2kcukr3/fn6qf9S+S^M
uXRl03aK/UakDSXDInm/nXWLIlFj0WPr9NE3ni3tdPq1Ndx3otpixzQaiEkxhZiaX9AkWC2lh1gC^M
IcglF00aJEIaYHuJKUPX6fSfiDOVaEJHBL6tdCyBQtmc7jwsSb3SvAbG2tvnlnaK0snqIKbRQEyK^M
SXdMuVjcdSoul0LQdMQgD30SUGOIyQee7n83MZXa8rh6qr0mJW0FtgZyJpVIUq88Fpl/rKfnovNT^M
trRTFFpWBzGNBmJSTComi1w3AdoRTcr0YuoGva4zLKYeYQgSwEm9IQbaCXTnYUnWoiSUrN1GGFK2^M
Txxb2ilJx+Uhpik4OjF98/vfmH98+gf3+X9ffWG+/OgX5otf/tz85y9/nlxM/uFPg7sTdIHpxVS6^M
3lVM4b4OQju+8jumLYSdY74OzX8XcPf1OPN18/3psbqxZdJ36/E4O1K6tuMctrWTro8gbfKOaRqO^M
```

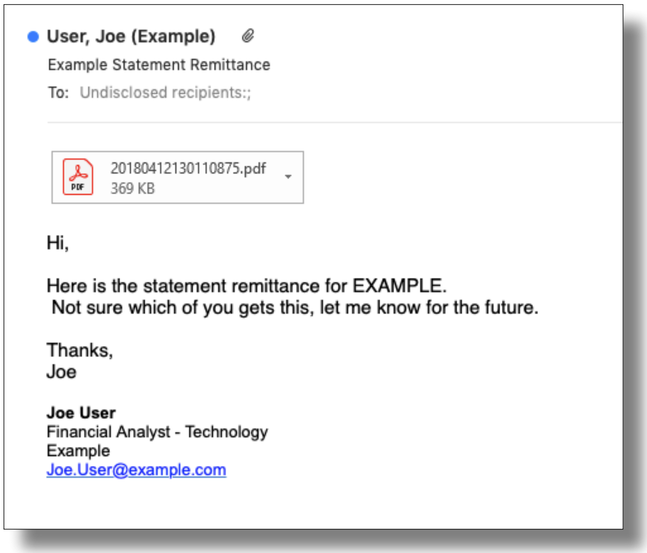
What we see here, in email-standards terms, is a *MIME part* with headers and a body. The Content-Type: image/png header means this is data for a Portable Network Graphic (PNG) image, and the data is encoded in Base64 coding in the fixed-width block of letters and numbers in the body.

One reason the attacker may have embedded the image this way instead of using a standard http:// link is that images embedded this way always display in the mail client, even when the *Display Remote Images* option is disabled. Why? Because this kind of image *isn't a remote image* — it's a local one! So the mail client assumes it must be safe. This means that even if your mail administrator disables remote images site-wide for your organization, you are still vulnerable to this kind of attack.

But clearly the primary deception here is that the sender of this email is trying to make it look like there is a PDF attachment to this mail that the user can open, when in fact the attachment icon itself is the image, and there is no real PDF attachment. So what's the point of this ruse?

If you look closely at the HTML you'll see that the <img> tag for the image actually appears within a <a>...</a> sequence, which denotes an *anchor* (hyperlink). This makes the image clickable, and it surely comes as no surprise that the href attribute on the <a> tag — the URL the user will be taken to upon clicking — is a malicious site impersonating SharePoint. Upon click-through, the user is prompted to enter credentials; this is a *credential harvesting* operation. Once the attacker has the victim's credentials, of course, he can impersonate that user on any O365 service, to steal PII... or send more phishing emails!

Here's another version of the same attack:



● **User, Joe (Example)**

Example Statement Remittance

To: Undisclosed recipients:;

Hi,

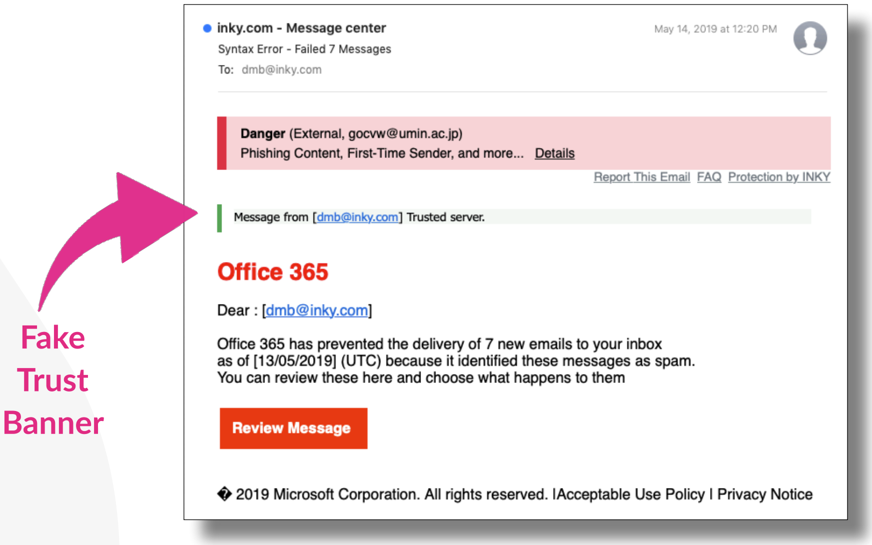
Here is the statement remittance for EXAMPLE.
Not sure which of you gets this, let me know for the future.

Thanks,
Joe

Joe User
Financial Analyst - Technology
Example
Joe.User@example.com

Under the hood, this one is very similar, but as you can see the attacker has made the fake attachment icon look slightly different, targeting users of another common mail client. But this one directs the victim to a phishy page hosted on sendgrid.net; attackers often like to use shared infrastructure like SendGrid to make their URLs look less phishy, both to human victims and to mail protection software that performs analysis on the URL text.

A related variant has attackers including fake trust banners in emails:



inky.com - Message center
Syntax Error - Failed 7 Messages
To: dmb@inky.com

May 14, 2019 at 12:20 PM

Danger (External, gocvw@umin.ac.jp)
Phishing Content, First-Time Sender, and more... Details

Report This Email FAQ Protection by INKY

Message from [dmb@inky.com] Trusted server.

Office 365

Dear : [dmb@inky.com]

Office 365 has prevented the delivery of 7 new emails to your inbox
as of [13/05/2019] (UTC) because it identified these messages as spam.
You can review these here and choose what happens to them

� 2019 Microsoft Corporation. All rights reserved. IAcceptable Use Policy I Privacy Notice

Fake Trust Banner

The red banner here was added by INKY; it means INKY classified the mail as definitely malicious. (Customers can configure these to go straight to quarantine.) But notice the green banner below it? That was added by the attacker: “Message from Trusted server.” — well, not so much! Here again, the attacker is mimicking a UI element in a common mail client to deceive the intended victim. Only in this case it’s to make the mail look more legitimate.

The INKY Solution: Spot the Fakes

So how do we deal with this? The answer is computer vision.

You may have read in other articles about INKY that we use computer vision techniques to spot brand forgery emails. In a nutshell, we train models on brand-indicative imagery, colors, text, and layout features. So INKY learns to recognize when a mail looks like it's from Microsoft, much like a person does. We've invested heavily in this technology to make it bulletproof.

And of course once you have a good hammer, everything tends to look like a nail — so we use this same computer vision capability to spot fake UI elements inserted into emails, by training models to recognize UI imagery instead of brand imagery. The details differ a bit, but the underlying concepts are the same.

The neat thing is that INKY can actually do *better* at this task than a human, because by parsing the MIME content of every email, INKY already distinguishes between embedded images and images added by the mail client itself. In fact, INKY *doesn't even see* the real UI elements added by the mail client — so in a very real sense this attack specifically exploits the human victim's inability to see the boundary between the UI imagery and the imagery in the mail itself.

Obviously when we spot a fake UI element in an email, that's a clear sign of malicious intent, meriting a red INKY banner and potential quarantine.

Other Countermeasures

You can take steps to protect yourself against this kind of attack even if you’re not yet an INKY customer. The simplest way is to enable “dark mode” in your mail client if it supports it. The embedded fake UI elements attackers are using (so far at least) all assume the email is displayed on a white background. In dark mode, the mail client sets the mail background to black and the fake UI element sticks out like a sore thumb.

You can also distinguish a fake attachment icon from a real one by hovering over the image. A real attachment icon will produce a tooltip with just the attachment file name. A fake one will yield a tooltip that looks like a standard http:// or https:// URL; no real attachment will ever have a name beginning with a URL scheme like that.

Conclusion

We know attackers will continue to up their game; we're sure to see ever more clever ways for scammers to hide from mail protection software like INKY Phish Fence. Our philosophy is to develop generalized countermeasures against entire classes of attacks, rather than playing "whack-a-mole" with threat feeds.

One class of attacks we've seen recently involves fake attachments and other UI elements embedded into emails. Hopefully we've given you some intuition about how these scams work and how INKY thwarts them.

We're passionate about email.

Ready to talk about an issue you're faced with in email security at your organization?

Request a demo today

www.inky.com

INKY

Understanding Phishing:

Fake Attachments

Executive Brief | Dave Baggett, INKY Founder and CEO