The Daily Scam Newsletter - January 30, 2019

The Week in Review

Last week our Top Story was about a rise in “sextortion scams.” We even showed readers that Doug and David received seven extortion emails claiming to release an embarrassing video that we know doesn’t exist! True to the scammer’s word, 72 hours after we received the first extortion threats, the “anonymous hacker” sent us a follow up email with his “last warning” to ruin our social life if we didn’t pay up. However, if you read the “PS” at the bottom of his email, you’ll see that he was kind enough to give us a 48 hour extension! How very kind of him, we’ll take it!

Subject: This is my last warning [redacted]@thedailyscam.com!
From: "Anonymous Hacker - Waltraud" <waltraud529@a.anonymous-observer.gq>
Date: Mon, January 21, 2019 1:19 am
To: [redacted]@thedailyscam.com

LAST WARNING [redacted]@thedailyscam.com!

You have the last chance to save your social life - I am not kidding!!

I give you the last 72 hours to make the payment before I send the video with your masturbation to all your friends and associates.

The last time you visited a erotic website with young Teens, you downloaded and installed the software I developed.

My program has turned on your camera and recorded your act of Masturbation and the video you were masturbating to. My software also downloaded all your email contact lists and a list of your Facebook friends.

I have both the '[redacted].mp4' with your masturbation and a file with all your contacts on my hard drive.
You are very perverted!

If you want me to delete both files and keep your secret, you must send me Bitcoin payment. I give you the last 72 hours. If you don't know how to send Bitcoins, visit Google.

Send 2000 USD to this Bitcoin address immediately: 38wAedEH2shqn7qe8GeM6WrokMhLFU1weT
(copy and paste)

1 BTC = 3470 USD right now, so send exactly 0.583981 BTC to the address above.
Do not try to cheat me! As soon as you open this Email I will know you opened it. This Bitcoin address is linked to you only, so I will know if you sent the correct amount. When you pay in full, I will remove both files and deactivate my software.

If you don't send the payment, I will send your masturbation video to ALL YOUR FRIENDS AND ASSOCIATES from your contact list I hacked.

Here are the payment details again: Send 0.583981 BTC to this Bitcoin address:

38wAedEH2shqn7qe8GeM6WrokMhLFU1weT

You can visit the police but nobody will help you.
I know what I am doing.
I don't live in your country and I know how to stay anonymous.

Don't try to deceive me - I will know it immediately - my spy ware is recording all the websites you visit and all keys you press. If you do - I will send this ugly recording to everyone you know, including your family.

Don't cheat me! Don't forget the shame and if you ignore this message your life will be ruined.

I am waiting for your Bitcoin payment.

Waltraud
Anonymous Hacker

P.S. If you need more time to buy and send 0.583981 BTC, open your notepad and write '48h plz'. I will consider giving you another 48 hours before I release the vid, but only when I really see you are struggling to buy bitcoin.

Our readers know how important we believe education is to help you reduce our online risks. This education also includes staying informed about the ways that your email and passwords have been captured and misused. The best online resource collecting data about known security breaches and enabling visitors to search the data is the website called **"Have I Been Pawned?"** We strongly recommend that you visit this website and enter all of your email addresses to see if they have ever been "pawned." If so, the website will tell you what it knows about the data breach, including whether or not passwords had been captured, when it happened and what some of the risks may be.

Phish Nets: JPMorgan Chase Bank and ATT Services

"Dear User. We are unable to verify some of your information" This phishing email for JPMorgan Chase account holders is pretty lame! In fact, it was so obviously a scam that the website hosting the phishing page was taken down within a few hours after the email came out. The link associated with "UPDATE" points to a link-shortening service. We couldn't see the final destination because it was removed so quickly. We wish all phish were this stupid.

From: Chase Online [mailto:goldcath@cox.net]
Sent: Saturday, January 05, 2019 8:50 PM
Subject: Alert

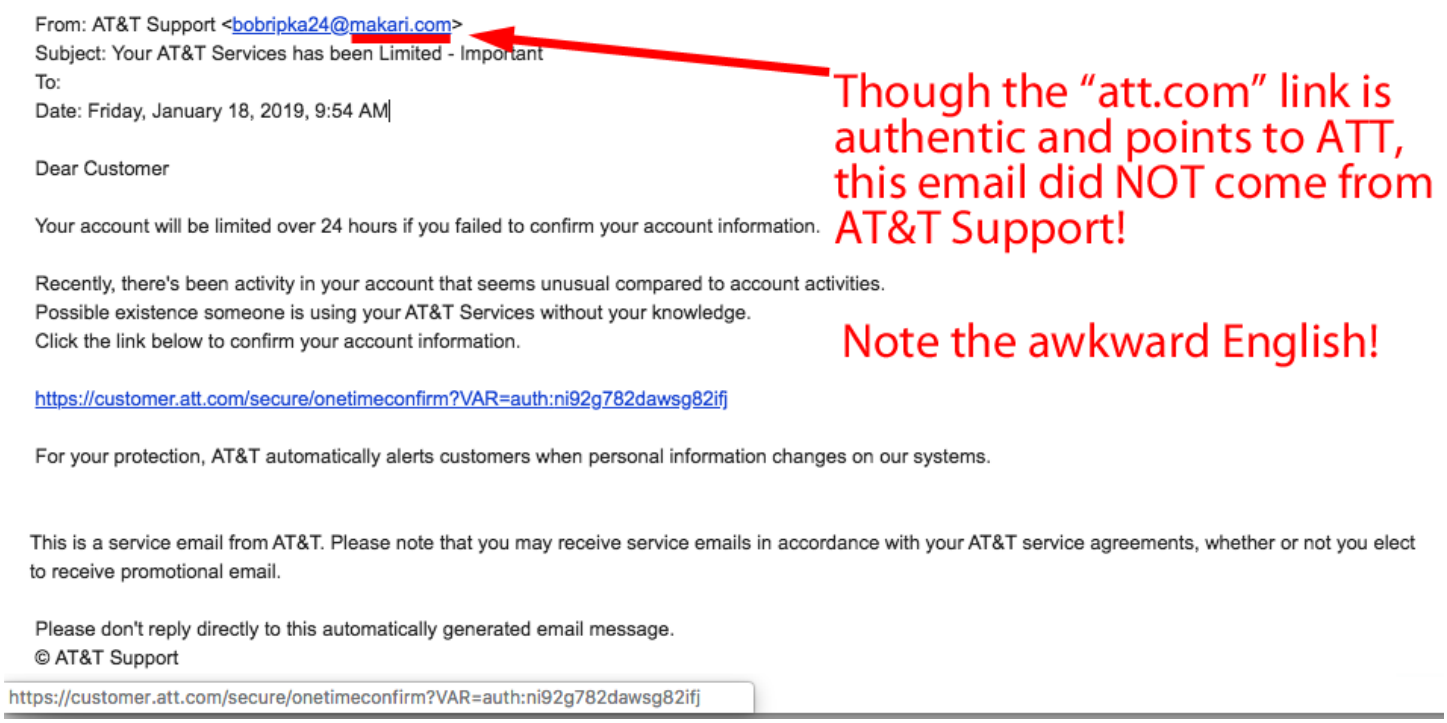
Dear User.

We are unable to verify some of your information
Update them now to avoid account restriction.

UPDATE
© 2018 JPMorgan Chase & Co. All rights reserved

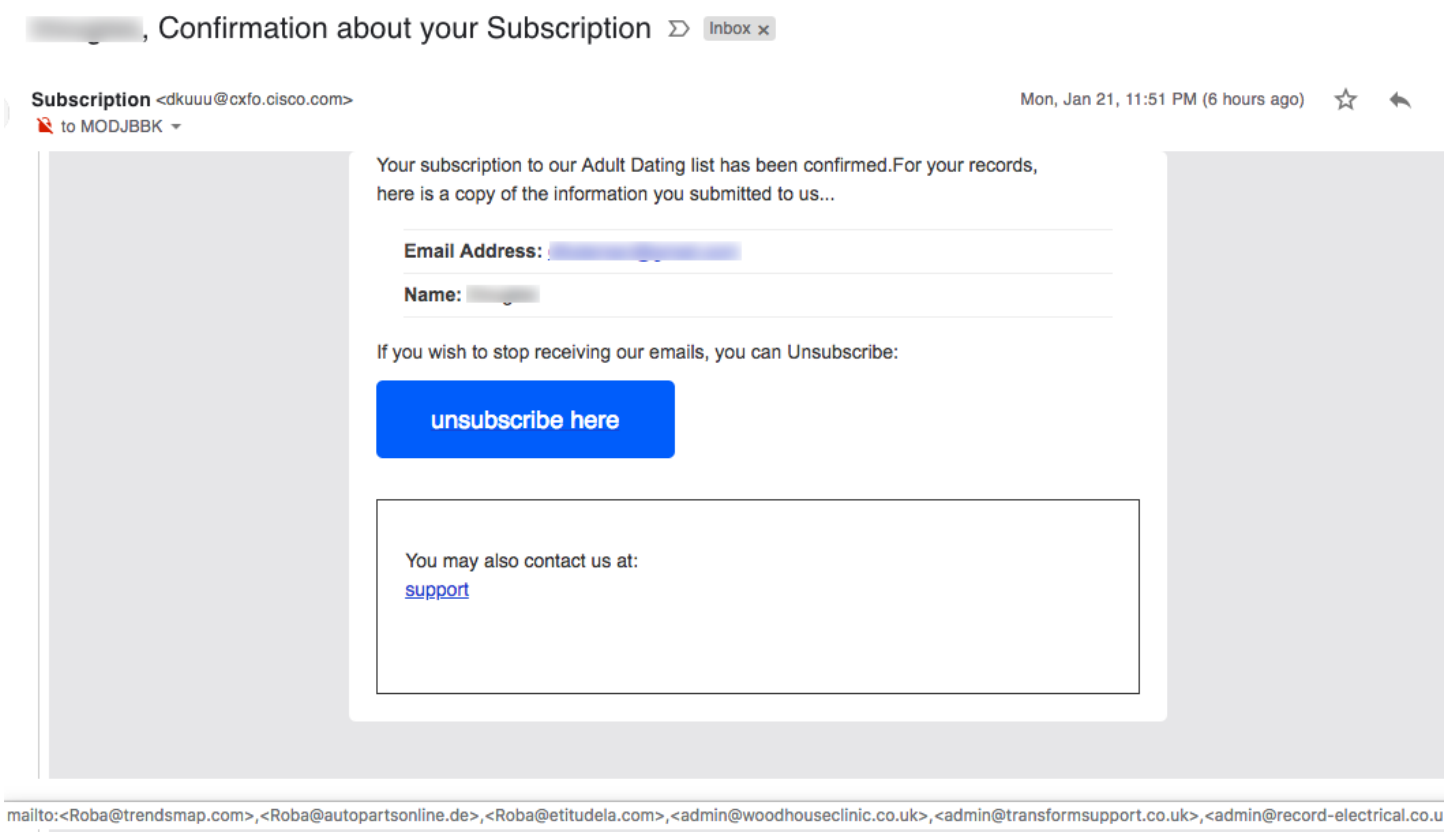
x.co/w34ty

Speaking of stupid… It appears to us that the criminals who sent this next malicious email disguised as an AT&T notification completely forgot to alter the link that they intended victims to click! The link is a legitimate one pointing correctly to ATT.com. And yet, if you look at the FROM address and read the email itself, there is no doubt that it wasn't created by AT&T Support.



Your Money: Confirmation About Your Subscription to Adult Dating Site
Apparently, we subscribed to an "Adult Dating list" according to an email sent to us! Part of the mystery here is that we have no idea what dating "list." This email confirmed our subscription by providing our email address and a first name as proof! How clever of them. We can stop receiving these emails by clicking the BIG BLUE BUTTON "unsubscribe here."

We're not quite sure what their game is but we know enough not to click the unsubscribe button. According to the behind-the-scenes coding, clicking that button will send a reply to the following email addresses around the world…
Roba "@" trendsmap.com (Hosted in Australia)
Roba "@" autopartsonline.de (Hosted in Germany)
Roba "@" etitudela.com (Hosted in France)
admin "@" woodhouseclinic.co.uk (Hosted in the United Kingdom)
admin "@" transformsupport.co.uk (Hosted in the United Kingdom)
admin "@" record-electrical.co.uk (Hosted in the United Kingdom)
admin "@" oxfordenglishexperience.co.uk (Hosted in the United Kingdom)



Top Story: Do You Pay Attention to Details?

One of the most important skills to help you stay safe online is to pay attention to details! This includes noticing when those details don't add up, or make sense. For example, we've seen cybercriminals misspell domain names in their effort to trick people with look-alike domains. Or they create domain names that "sound" official, but are not. Here are a few examples…

Amricanexprss[.com]
Paypai[.]com
Apple-authorize[.]info
Myappleid-secure[.]com

We wanted to present you with a small challenge this week, and hope you have fun at the same time. What follows is a very obvious scam email claiming to represent the multinational telecom company known as MTN. It informs the recipient that she or he has been selected to win $7 million U.S. dollars as part of a 2019 promotion. Read the email closely and critically. How many "red flags" (suspicions) can you cite because things don't "add up" or make sense? We count twelve! No doubt, some of our readers will find more. Our dirty dozen are listed below. If you find others we missed, please share them with us by emailing them to **spoofs@thedailyscam.com.**

This message is for the owner of this email address.

Angela Johnson <info.office2019@yahoo.com> Sat, Jan 19, 2019 at 6:02 AM
Reply-To: Angela Johnson <info.office2019@yahoo.com>

MTN GROUP LIMITED.

This message is for the owner of this email address.

Dear Lucky Recipient.

This is to officially announce to you that you was selected by your email address and Number 3 Lucky winners who won USD$ 7 Million United States Dollars on the MTN 18 Years Anniversary PROMOTION **2019**.Congratulations!.

MTN Group Limited,we are Mobile telecommunication company. If you never heard about MTN Group Limited please visit this website: https://en.wikipedia.org/wiki/MTN_Group

The online draws was conducted by a random selection of email addresses from an exclusive list of 29,031 E-mail addresses of individuals all over the world and corporate bodies picked by an advanced automated random computer search. The selection process was carried out through random selection in our computerized email selection machine (TOPAZ),People under the age of 18 years are not included.

With a great pleasure to bring to your notice this result from MTN Group Limited.

This is to inform you that MTN Group Limited,we are inviting you for Congratulations and to hand you over your funds immediately. Please,kindly contact Rev. Fred J. Williams,Head of Department,for more directives.

Rev.Fred J. Williams,
E-mail: file.officefile2016@yandex.com
P.O Box: 7754

NOTE: Federal Bureau of Investigations (F.B.I.) has investigated MTN Group Promotion Award and approved with Letter below to all you Beneficiaries.

Beneficiaries of MTN Group Limited.

U. S. Federal Bureau of Investigations (F.B.I.). We are officially informing you that MTN Group Limited Award has been thoroughly investigated by the U. S. Federal Bureau of Investigations.

According to the law defined in federal law 42 CFR 455.2 and 18 USC § 1030, provides that a company or Individuals, participating in Internet fraud may be found guilty of a felony and face a fine of up to $250,000 and/or up to 20 years in jail.

This is to inform all the beneficiaries of MTN Group that your Wining Prize from MTN Group Limited has been investigated and it is Genuine. U.S. Department of Justice.

MTN Group Limited Promo,the 5th of its kind to be held.Happy New Year!!

Sincerely
Mrs.Angela Johnson

MTN GROUP LIMITED.

https://mail.yandex.com/re.jsx?h=a,062ZOXsZzP_fXFRbDtkPQg&l=aHR0cHM6Ly9tYWlsLnlhbmRleC5jb20vc...ZoQ1dGWXhaREJoTVZWNVZHdGtXR0pyY0ZoWmExcDNZMnhTVjFkdVpGaFdiWFF6Vm0weE1GWXdNVVZTYm14YVRVZG9Wdw

I spy with my critical eye, the following suspicious things that have gone awry...

1. I've won $7 million dollars and the best they can do is address me as the *"owner of the email address?"*
2. The sender claims to represent the company MTN but her email address is from a yahoo account, not a MTN.com account.
3. Again, I am not addressed by name, just "Dear Lucky Recipient."
4. Don't you expect the English in this email to be flawless? "...you was selected by your email address" (We count 15 grammatical errors, errors of punctuation or capitalization, as well as awkward English.)
5. The only link on the page, identified as Wikipedia, leads to the email service **Yandex.com**. According to this REAL Wikipedia page, Yandex is a Russian company offering internet products and services across Eastern Europe, Russia and Africa, such as free email service.
6. Isn't it odd that the "Head of Department" (what department?) at MTN is a Reverend? ... Rev. Fred J Williams. Is he done tending his flock, or does he have to work two jobs to make ends meet?
7. The email address for Rev. Williams in not an mtn.com account, but a Yandex account again. Also, it is a very peculiar email address name... "file.officefile2016"
8. Why provide a Post Office Box for Rev. Williams but no other address information? Not even a city or country!

9. It is not the business of the FBI to "investigate" any promotion or award to determine authenticity or offer a stamp of approval. (And at the bottom of the email, the sender drops in “U.S. Department of Justice” as well, as if that will add some additional legitimacy to their claim.)
10. It is very odd that the winners of a company promotion should be called "beneficiaries." This is a term that typically refers to those who receive money from a trust, will or life insurance policy.
11. In an email to announce a $7 million dollar winner of a promotion for an International company, one would think that the email would use the same font and size throughout. Clearly, there was no marketing department doing their due diligence to make sure this email represented the company well. It is not professionally crafted!
12. The ONLY way to respond to this winning announcement is through email. THAT of and by itself means it is a scam!

A footnote to this exercise in critical reading skills...
We sometimes notice that cybercriminals will try to obfuscate a link by making it so terribly long it will not display properly when the recipient mouses over it. We’ve seen some really long links, including some with redirects hidden in them. But the link in this email exceeds anything we have ever seen before! Mousing over the link for the Wikipedia article, we discovered that it consists of 88,460 characters! Here is an image showing just the first couple of hundred characters:

MTN GROUP LIMITED.

This message is for the owner of this email address.

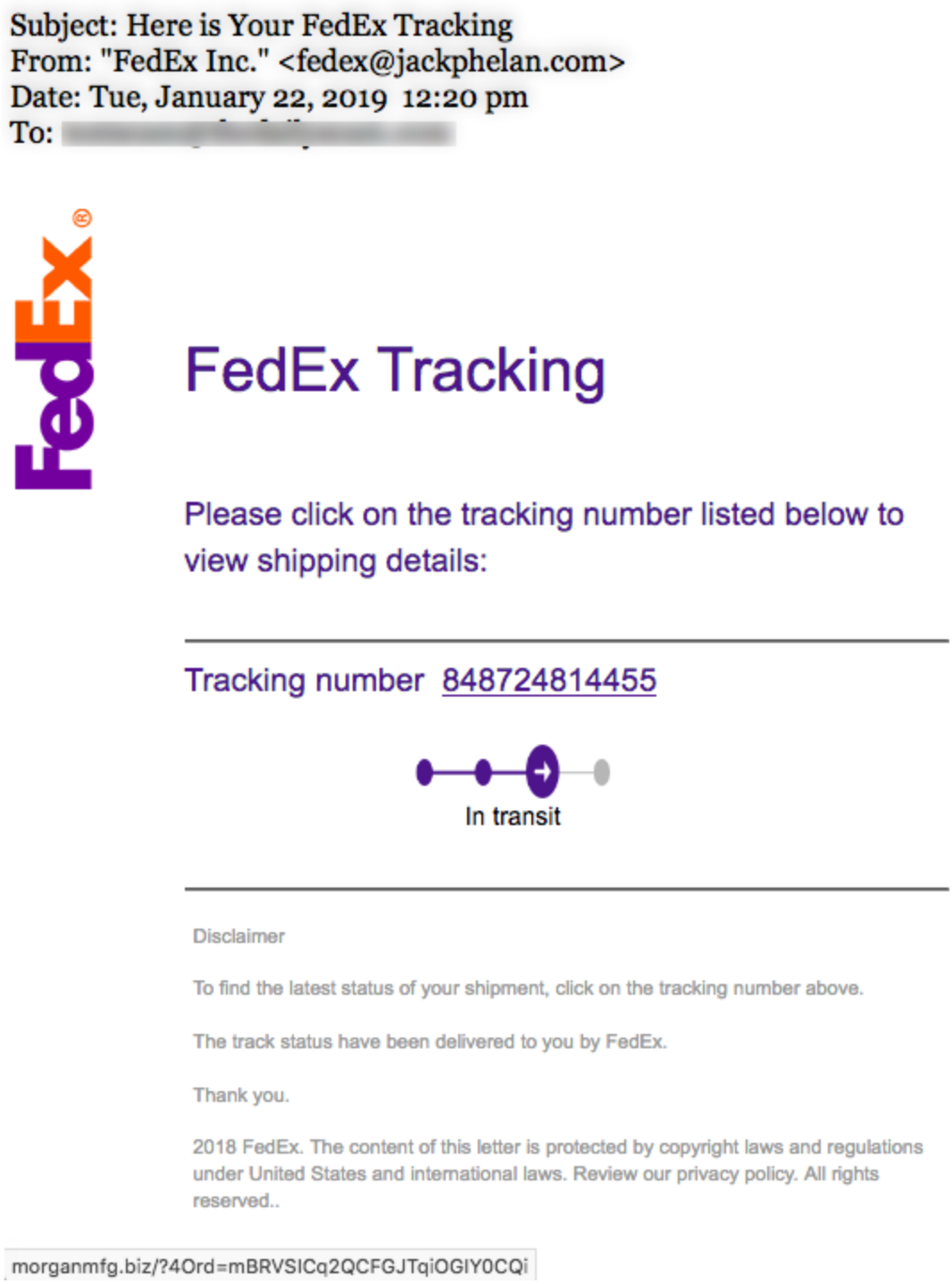
Dear Lucky Recipient.

This is to officially announce to you that you was selected by your email address and Number 3 Lucky winners who won USD$ 7 Million United States Dollars on the MTN 18 Years Anniversary PROMOTION **2019**.Congratulations!.

MTN Group Limited,we are Mobile telecommunication company. If you never heard about MTN Group Limited please visit this website: <a href="https://mail.yandex.com/re.jsx?h=a,062ZOXsZzP_fXFRbDtkPQg&l=aHR0cHM6Ly9tYWlsLnlhbmRleC5jb20vcmUuanN4P2g9YSw1LUtCNVlfc1pC
NW9wNkNzVXlzdHJnJmw9YUhSMGNITTZMeTl0WVdsc0xubGhibVJsZUM1amlyMHZjbVV1YW5ONFAyZzlZU3hhZW1SRl
ExTnBSVGREU2xGcFZrbHFOekU0ZWxCbkptdzlZVWhTTUdOSVRUWk1lVGwwV1Zkc2MweHViR2hpYlZKc1pVTTFhbUl5
TUhaamJWVjFZVzVPTkZBeVp6bFpVM2hTWVZSS05sRllZek5STWpGdVVsVnplbEZ0T1VoU2JWWm9Ua1JhUWtwdGR6bF
pWV2hUVFVkT1NWUlVXazFsVkd3d1YxWmtjMk13ZUhWaVlyaHBZbFpLYzFwVlRURmhiVWw1VFVoYWFtSldWakZaVnpW
UFRrWkJlVnA2YkZwVk0yUXpXV3haTlZSV1ZraFNWRVpoWWxSc1ZGbHROVU5TTWxaMFRWWktWMDB3V2s1V1ZscHpUVE
J3ZEdSNmJGcFdWMmhVVkZWa1QxTldVbFZYYXpGc1ZrZDNkMVl4V210ak1rMTNaVWhXYVZJeWFIQlpiRnBMWXpGd1Zs
UlVSbWhpVld3MVZGVm9ZV0Z0U2xkV2FrWmFWbnBXVUZScldrSmxWbkEyWWtad1ZrMHlhSFpXVmxKTFpERmFjMk5JVW
xSaE1EVnpWakJWTUUxV2EzbGxSM1JoWWtaYVdGa3dhRzlYYXpGV1UxaHNWazF1YUhwVlYzUjNaRWRTTm1KR2NGZFdN
bWhWVmtaV2ExUXhUbGRWYkZaWVlYcEdjMVpyWkROa01WbDRWMjEwYWsxck1UTmFWV2hYWVZaSmVXRklRbHBpUm5CTV
dYcEdkMVpzVWxWU2JXaHBWbGQzTVZaR1ZtOVpWMFowVTJ4a1YyRnJXbUZXYm5CWFZVWlNjbGRyU214V2JrRXlXV3Rh
ZDFack1IbGhSa3BYVjBoQ1JGWnFSbGRqTVdSWlkwWlNWMUpyY0hsV2JYUldaREpXVjJKR1pGZGlhelZ6Vm1wQ1YwNU
diSFZqUlRsWFZqQndTRlV5YzNoV1ZURkhWMnhvVjFZelVqTmFSV1JUVG0xS1IyTkdaRmROYldoV1ZtdGFWMkV4VVho
VWJHUldZa1phV1ZsWWNFZGpNVnB5V2tST2EwMVdiRFJXTWpFd1lXc3hjazFVVG1GV1YyaFlXVlphU21WWFJrbFJiSE

For Your Safety: Your FedEx Tracking Number and Critical Update Available
And while we’re on the topic of “paying attention to details” check out these next two emails. Both lead directly to a malware infection! The first may say “here is your FedEx tracking” but it clearly didn’t come from

fedex.com. A mouse-over of the tracking number in this email shows that it points to a website that appears to be for a business called “Morgan Manufacturing.” However, this is not the real website for Morgan Manufacturing. And waiting for you at the end of that link is some nasty malware!


Subject: Here is Your FedEx Tracking
From: "FedEx Inc." <fedex@jackphelan.com>
Date: Tue, January 22, 2019 12:20 pm
To:

FedEx Tracking

Please click on the tracking number listed below to view shipping details:

Tracking number 848724814455

In transit

Disclaimer

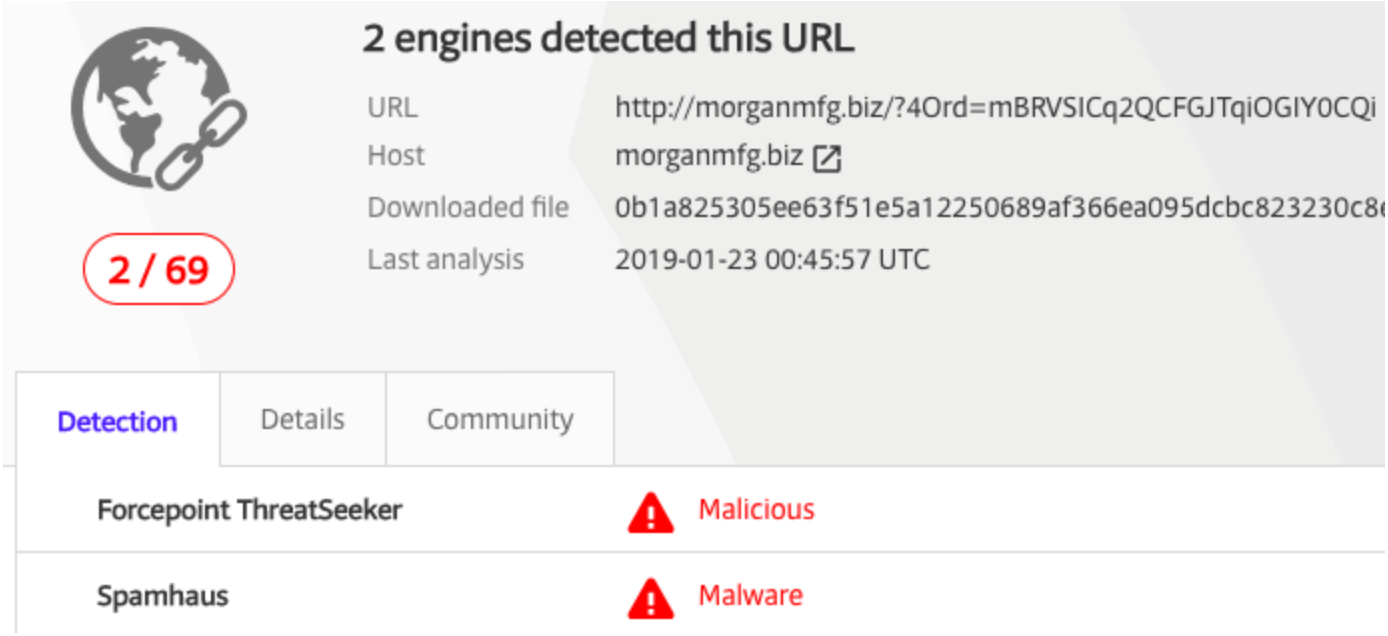
To find the latest status of your shipment, click on the tracking number above.

The track status have been delivered to you by FedEx.

Thank you.

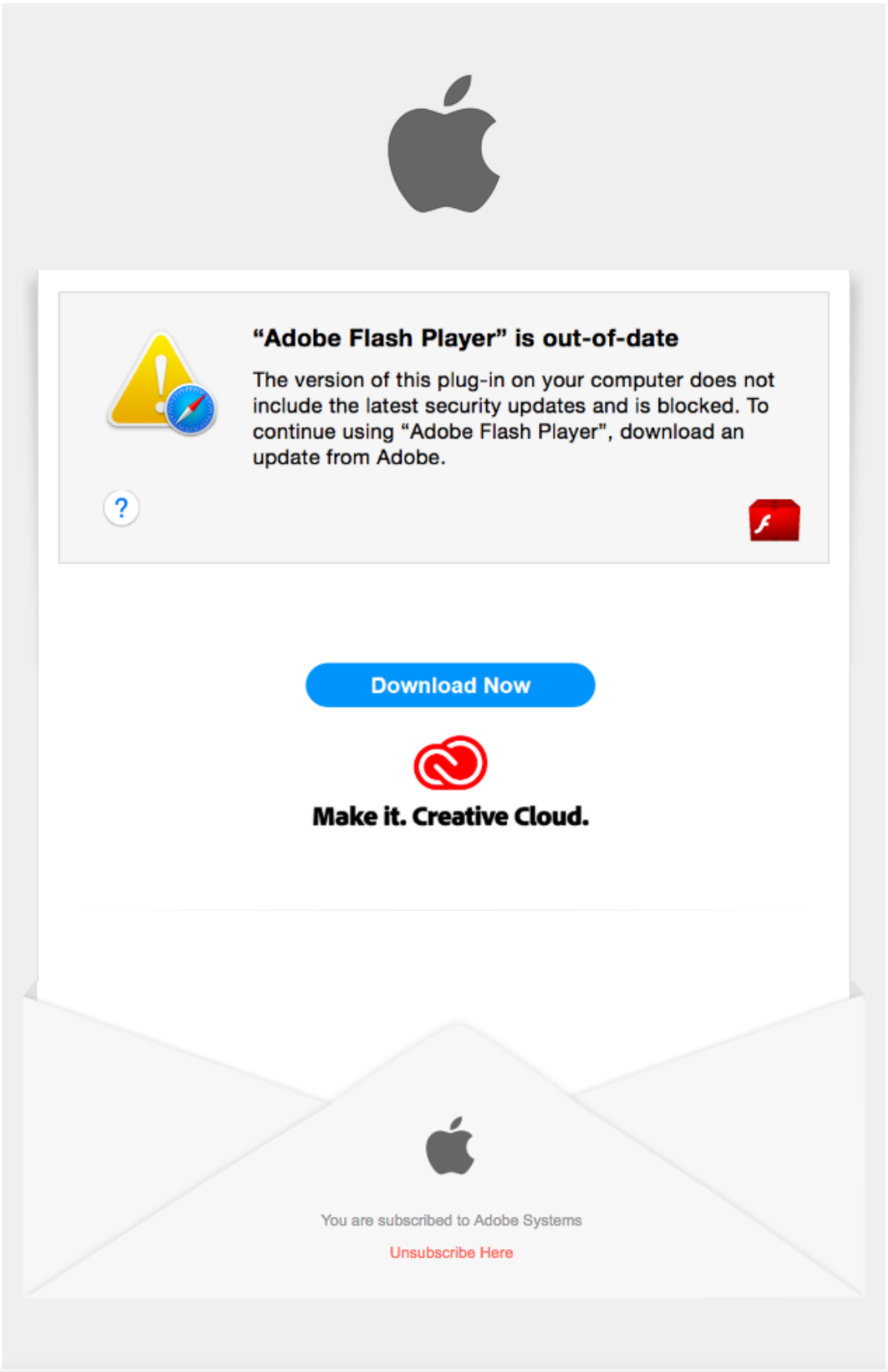
2018 FedEx. The content of this letter is protected by copyright laws and regulations under United States and international laws. Review our privacy policy. All rights reserved..

morganmfg.biz/?4Ord=mBRVSICq2QCFGJTqiOGIY0CQi



This next email claims to represent Adobe software but is far from it! It came from a domain in the European Union with links pointing back to that malicious domain. This is clickbait to have you install malware disguised as Adobe flash software. Just delete!

From: Adobe Systems <info@wintersales.eu>
Subject: Critical Update available for macOS Adobe Flash Player (highly recommended)
Date: January 21, 2019 at 00:08:33 PST
To: "[redacted]" <[redacted]>
Reply-To: Adobe Systems <info@wintersales.eu>



Until next week, surf safely!

info@thedailyscam.com

Free Newsletter Every Wednesday