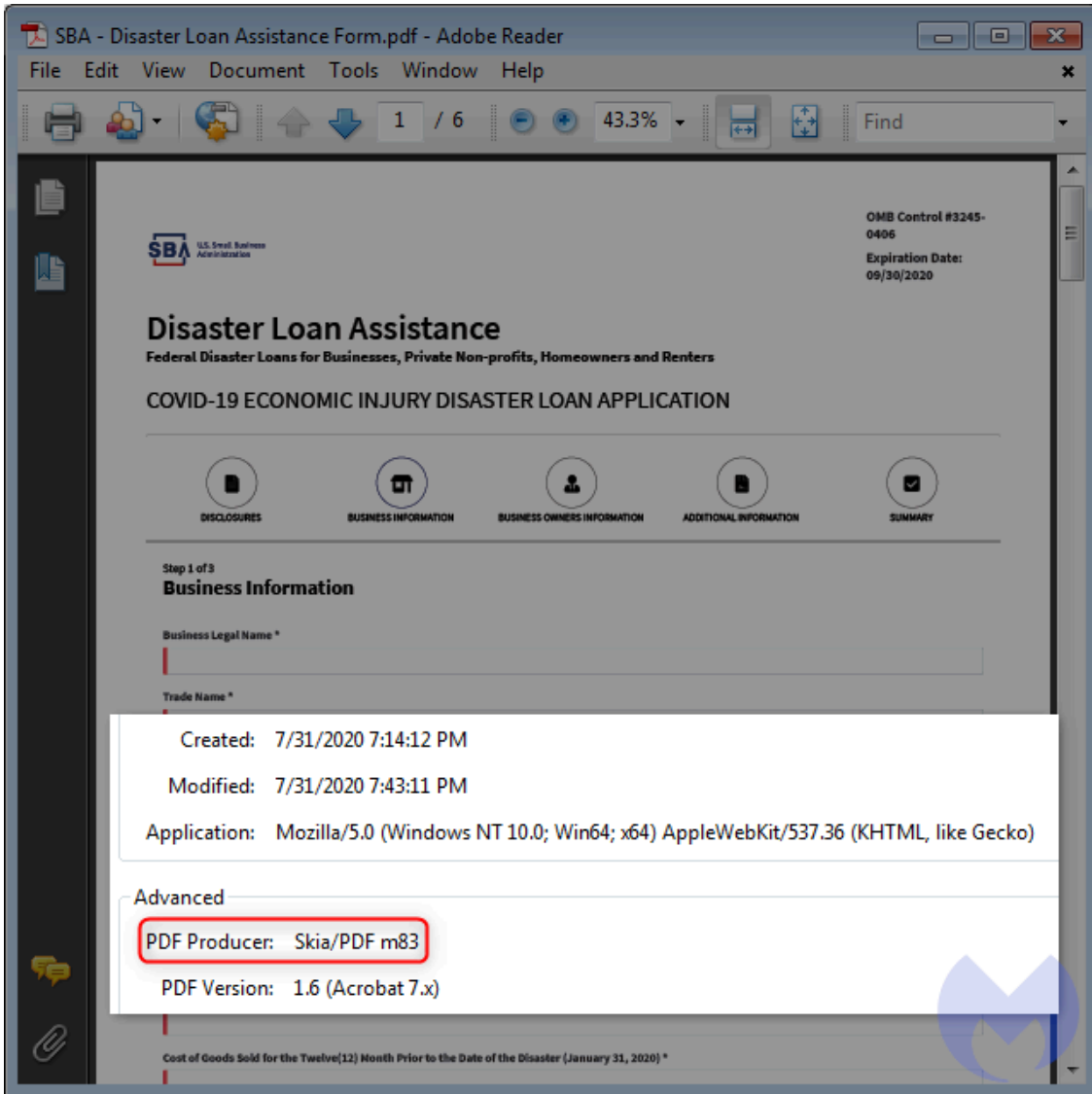


SBA phishing scams: from malware to advanced social engineering

| Malwarebytes Labs

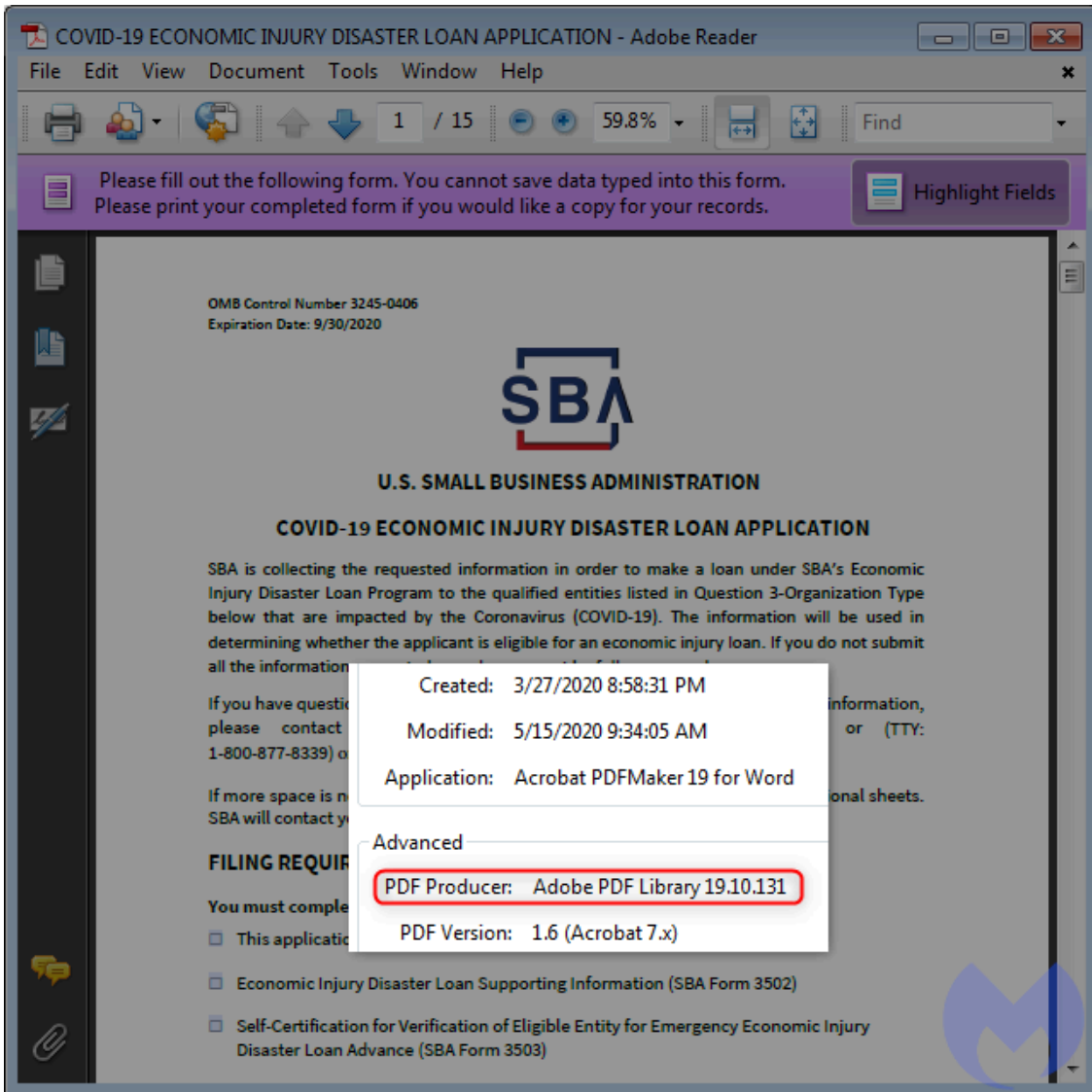
By Jérôme Segura

Published: 2020-08-09 · Archived: 2026-04-05 13:48:48 UTC



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~
Domain Name: gov-sba.us
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF4235C-NSR
Registrar WHOIS Server:
Registrar URL: www.psi-usa.info
Updated Date: 2020-08-05T06:22:13Z
Creation Date: 2020-07-31T06:22:09Z
Registry Expiry Date: 2021-07-31T06:22:09Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr
ansferProhibited
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR
Registrant Name: Krikor Derabrahamian
Registrant Organization:
Registrant Street: Rotenloewengasse 15
Registrant Street:
Registrant Street:
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

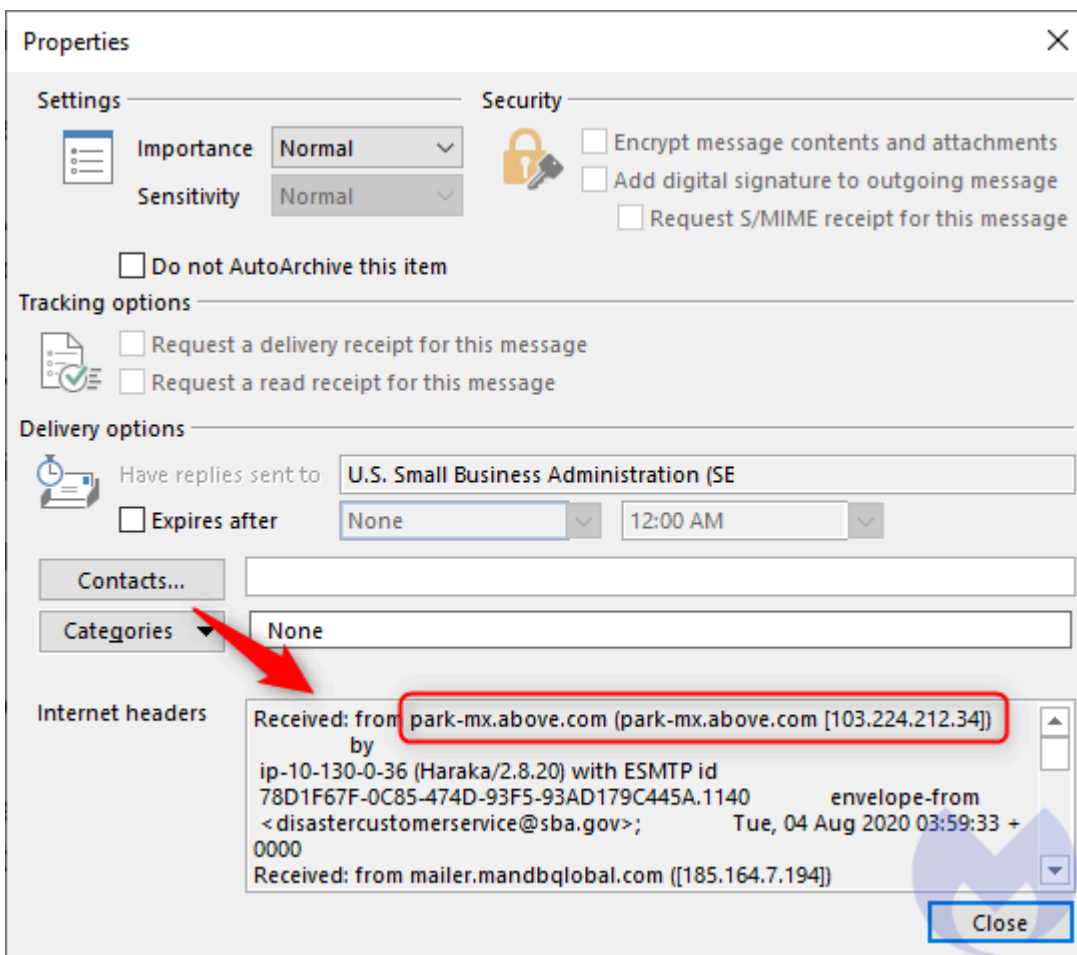
There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to [phishing](#) emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

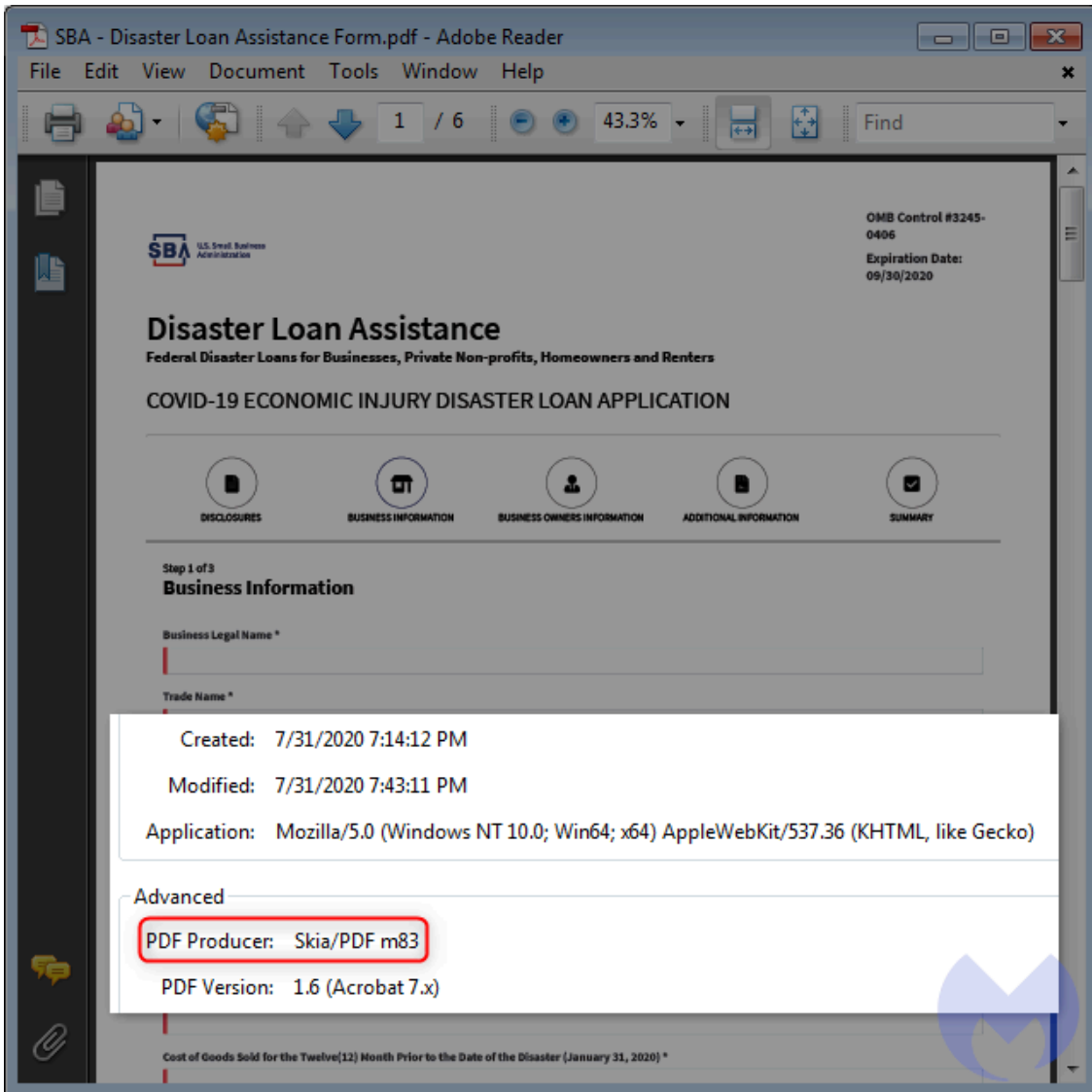
Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

[Malwarebytes](#) also protects against phishing attacks and malware by blocking offending infrastructure used by scammers.



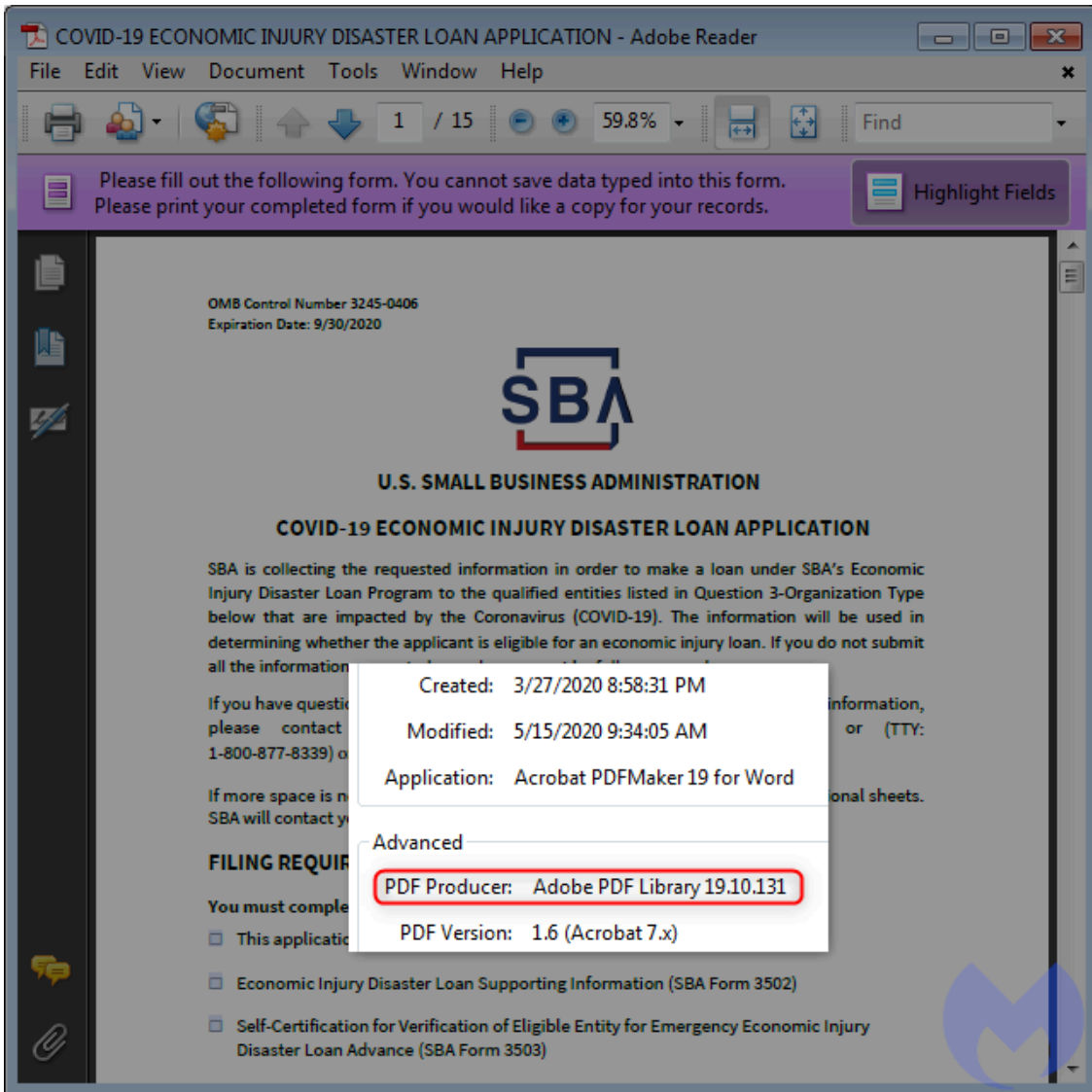
One of the items to look at is the “Received” field. In this case, it shows a hostname (park-mx.above[.]com) that looks suspicious. In fact, we can see it has already been mentioned in [another scam campaign](#).

If we go back to this email, we see that it contains an attachment, a loan application with the 3245-0406 reference number. A look at the PDF metadata can sometimes reveal interesting information.



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~
Domain Name: gov-sba.us
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF0F4235C-NSR
Registrar WHOIS Server:
Registrar URL: www.psi-usa.info
Updated Date: 2020-08-05T06:22:13Z
Creation Date: 2020-07-31T06:22:09Z
Registry Expiry Date: 2021-07-31T06:22:09Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr
ansferProhibited
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR
Registrant Name: Krikor Derabrahamian
Registrant Organization:
Registrant Street: Rotenloewengasse 15
Registrant Street:
Registrant Street:
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

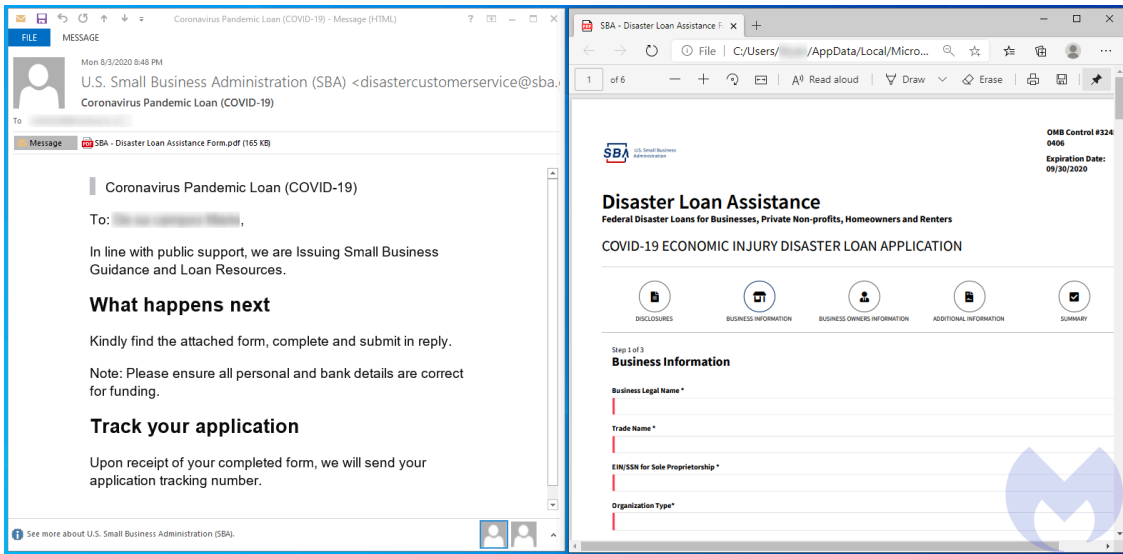
There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to phishing emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

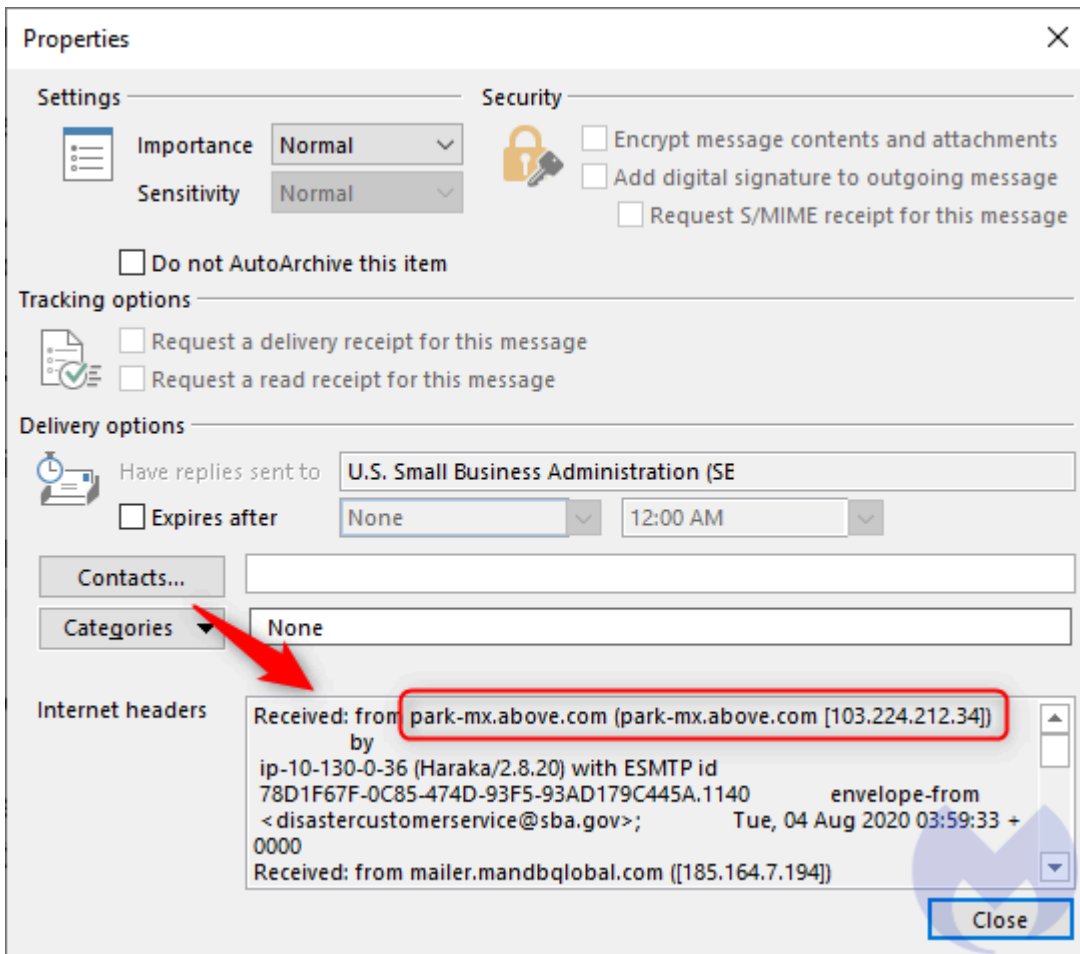
[Malwarebytes](#) also protects against phishing attacks and [malware](#) by blocking offending infrastructure used by scammers.



This latest campaign started in early August and is convincing enough to fool even seasoned security experts. Here’s a closer look at some red flags we encountered as we analyzed it.

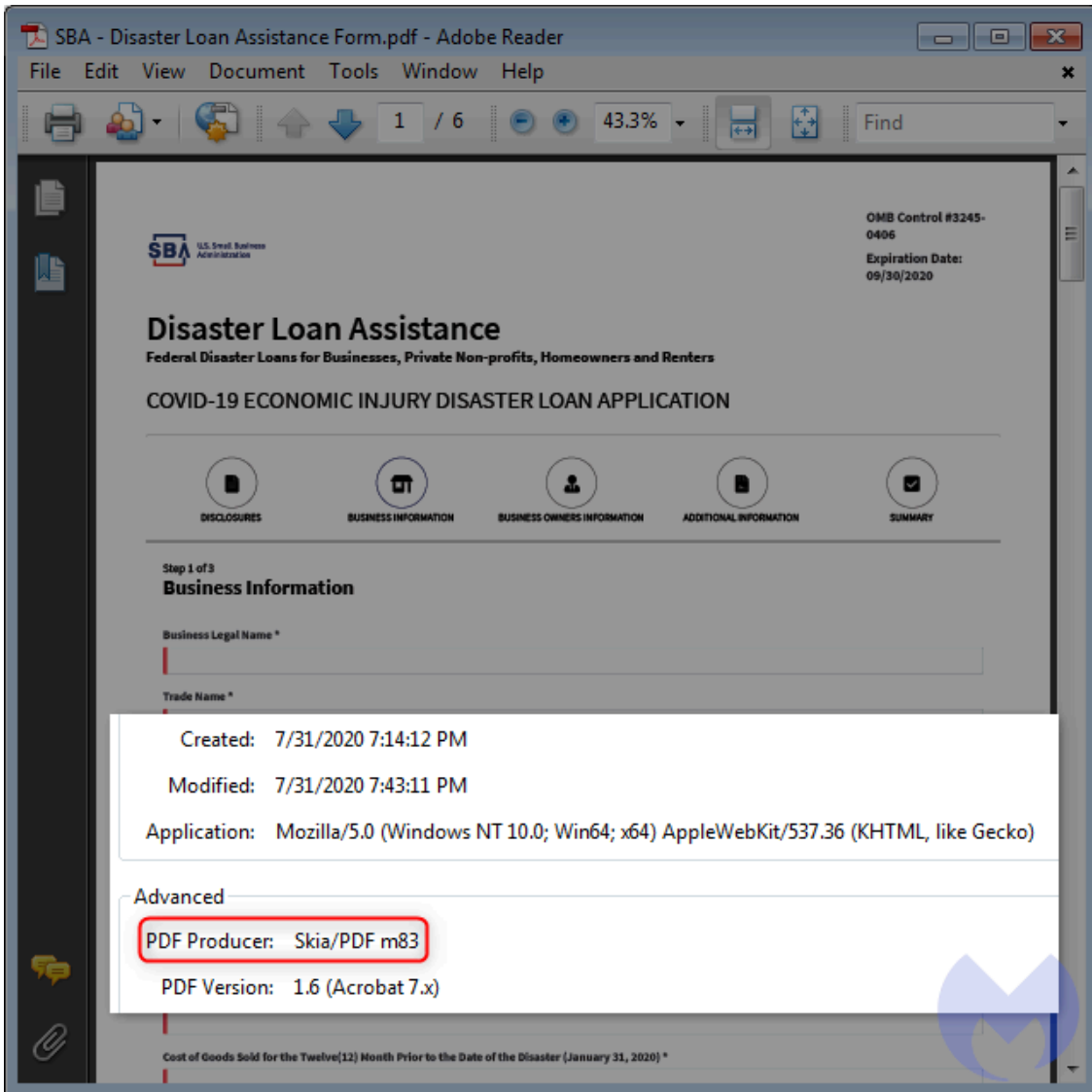
Most people aren’t aware of [email spoofing](#), and believe that if the sender’s email matches that of a legitimate organization, it must be real. Unfortunately, that is not the case, and there are additional checks that need to be performed to confirm the authenticity of a sender.

There are various technologies for confirming the true sender email address, but we will instead focus on the emails headers, a sort of blue print that is available to anyone. Depending on the email client, there are different ways to view such headers. In Outlook, you can click File and then Properties to display them:



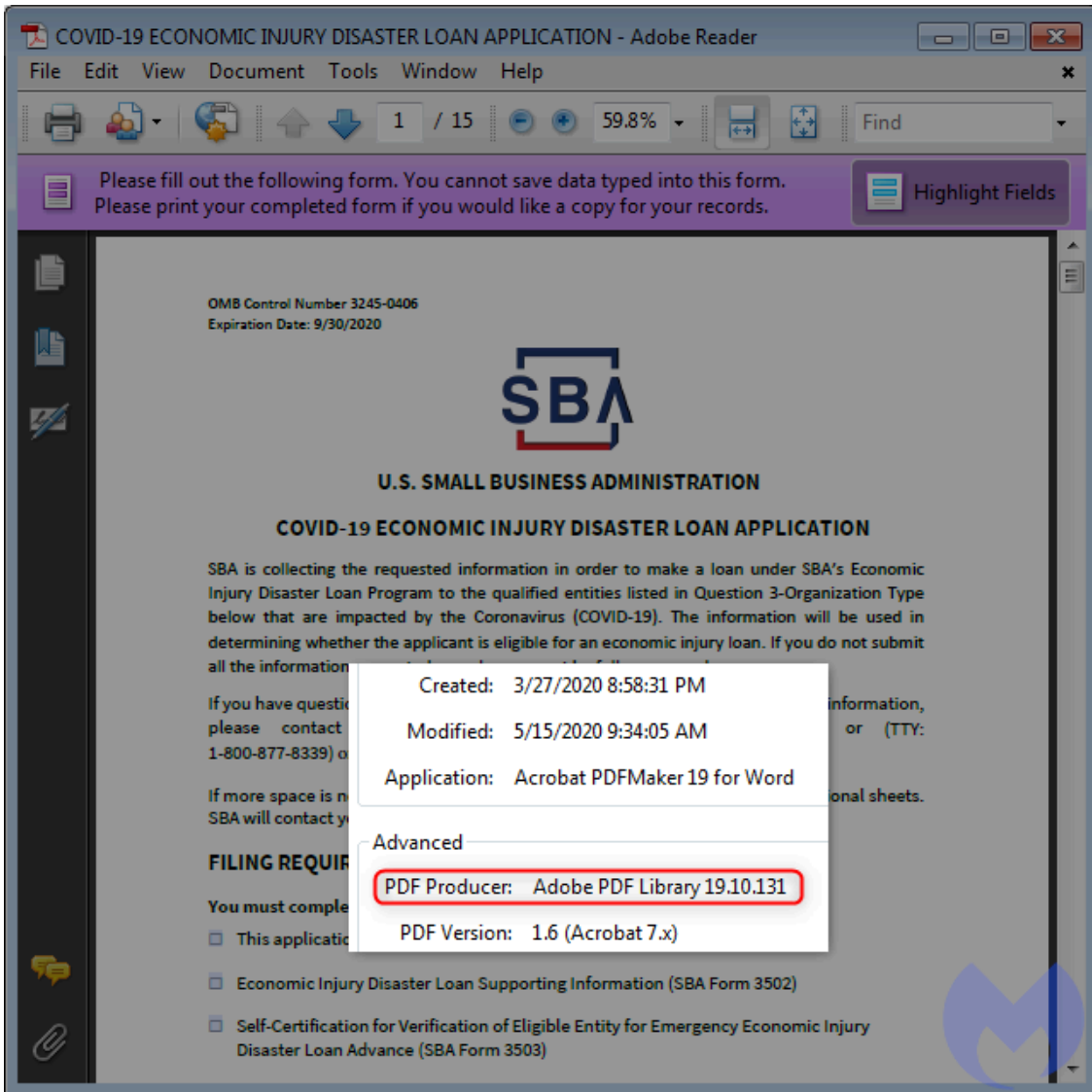
One of the items to look at is the “Received” field. In this case, it shows a hostname (park-mx.above[.]com) that looks suspicious. In fact, we can see it has already been mentioned in [another scam campaign](#).

If we go back to this email, we see that it contains an attachment, a loan application with the 3245-0406 reference number. A look at the PDF metadata can sometimes reveal interesting information.



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~  
Domain Name: gov-sba.us  
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF4235C-NSR  
Registrar WHOIS Server:  
Registrar URL: www.psi-usa.info  
Updated Date: 2020-08-05T06:22:13Z  
Creation Date: 2020-07-31T06:22:09Z  
Registry Expiry Date: 2021-07-31T06:22:09Z  
Registrar: PSI-USA, Inc. dba Domain Robot  
Registrar IANA ID: 151  
Registrar Abuse Contact Email:  
Registrar Abuse Contact Phone:  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr  
ansferProhibited  
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR  
Registrant Name: Krikor Derabrahamian  
Registrant Organization:  
Registrant Street: Rotenloewengasse 15  
Registrant Street:  
Registrant Street:  
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

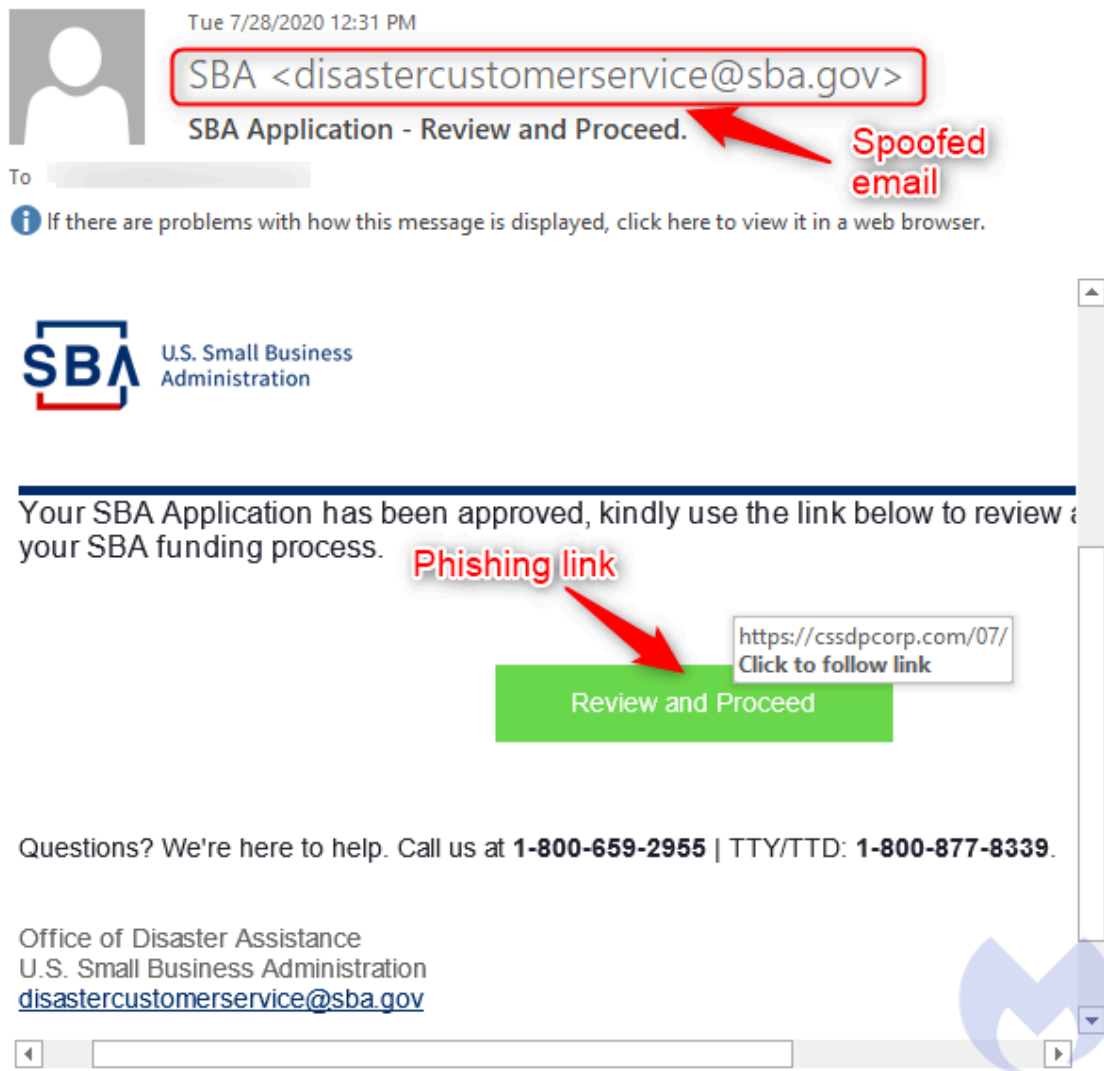
There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to phishing emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

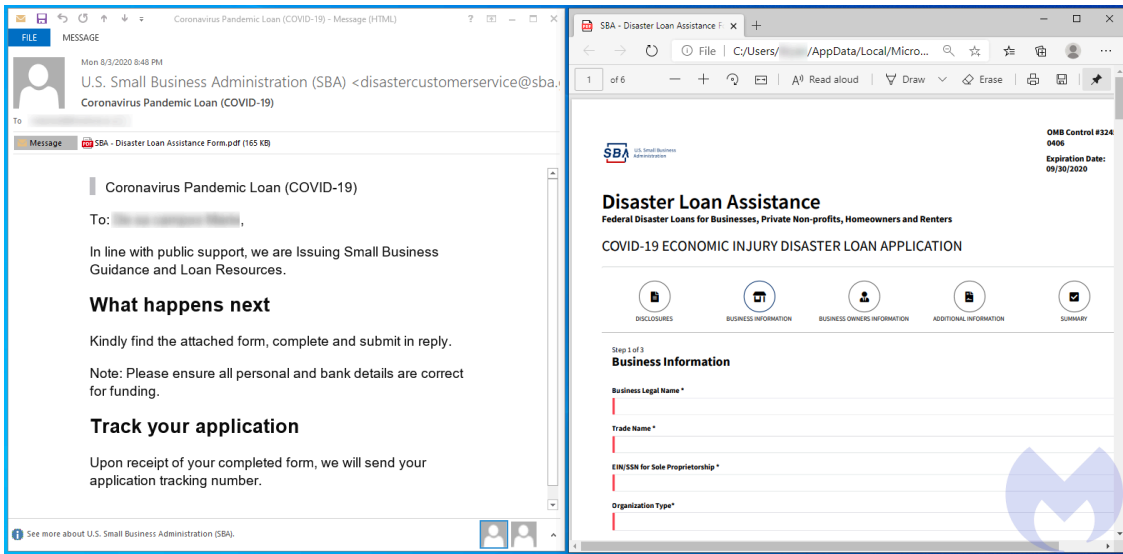
[Malwarebytes](#) also protects against phishing attacks and malware by blocking offending infrastructure used by scammers.



A URL, especially if it has nothing to do with the sender, is a big giveaway that the email may be fraudulent. But things get a little more complicated when attackers are using attachments that look seemingly legitimate.

Advanced phishing attempt

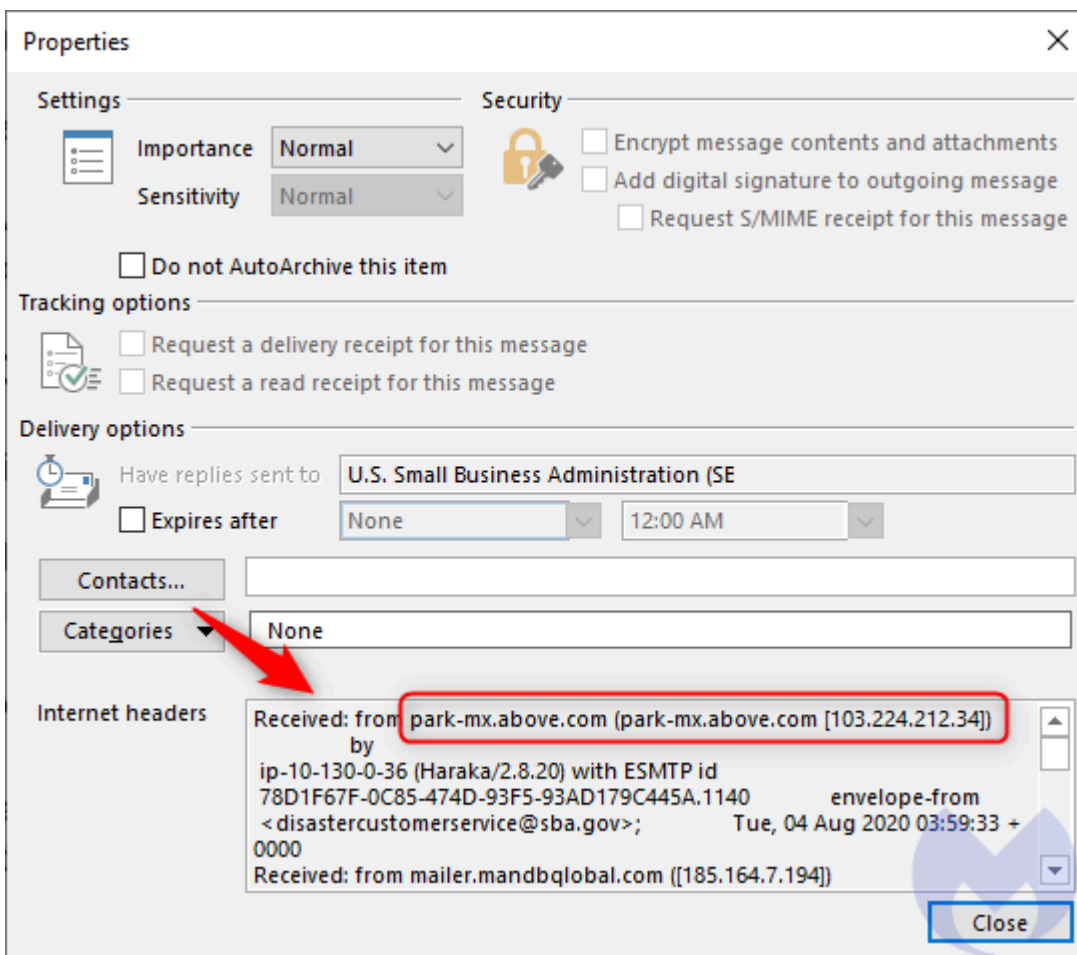
This is what we saw in a pretty clever and daring scheme that tricks people into completing a full form containing highly personal information, including bank account details. These could be used to directly drain accounts or in an additional layer of social engineering, which tricks users into paying in advanced fees that don't exist as part of the real SBA program.



This latest campaign started in early August and is convincing enough to fool even seasoned security experts. Here’s a closer look at some red flags we encountered as we analyzed it.

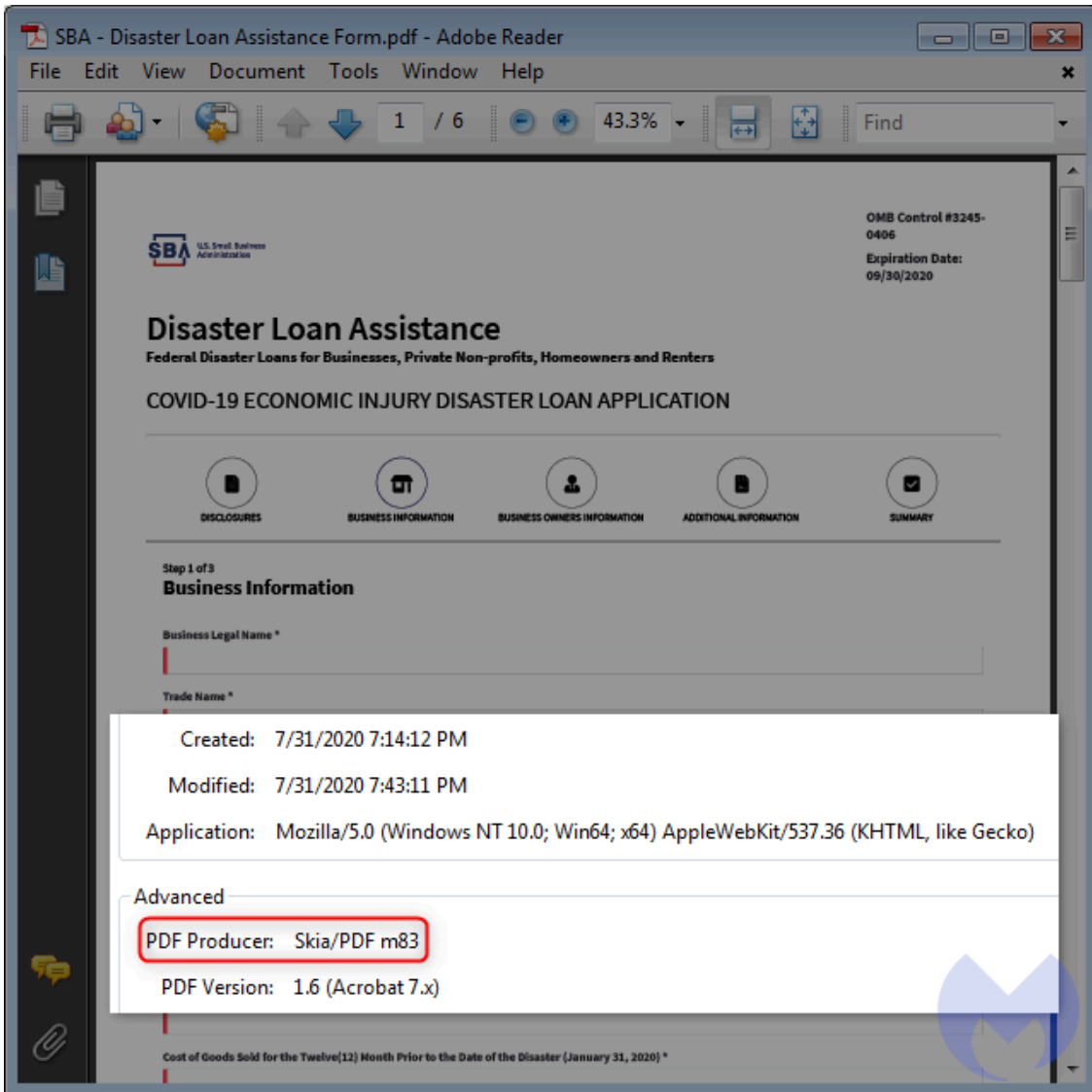
Most people aren’t aware of [email spoofing](#) and believe that if the sender’s email matches that of a legitimate organization, it must be real. Unfortunately, that is not the case, and there are additional checks that need to be performed to confirm the authenticity of a sender.

There are various technologies for confirming the true sender email address, but we will instead focus on the emails headers, a sort of blue print that is available to anyone. Depending on the email client, there are different ways to view such headers. In Outlook, you can click File and then Properties to display them:



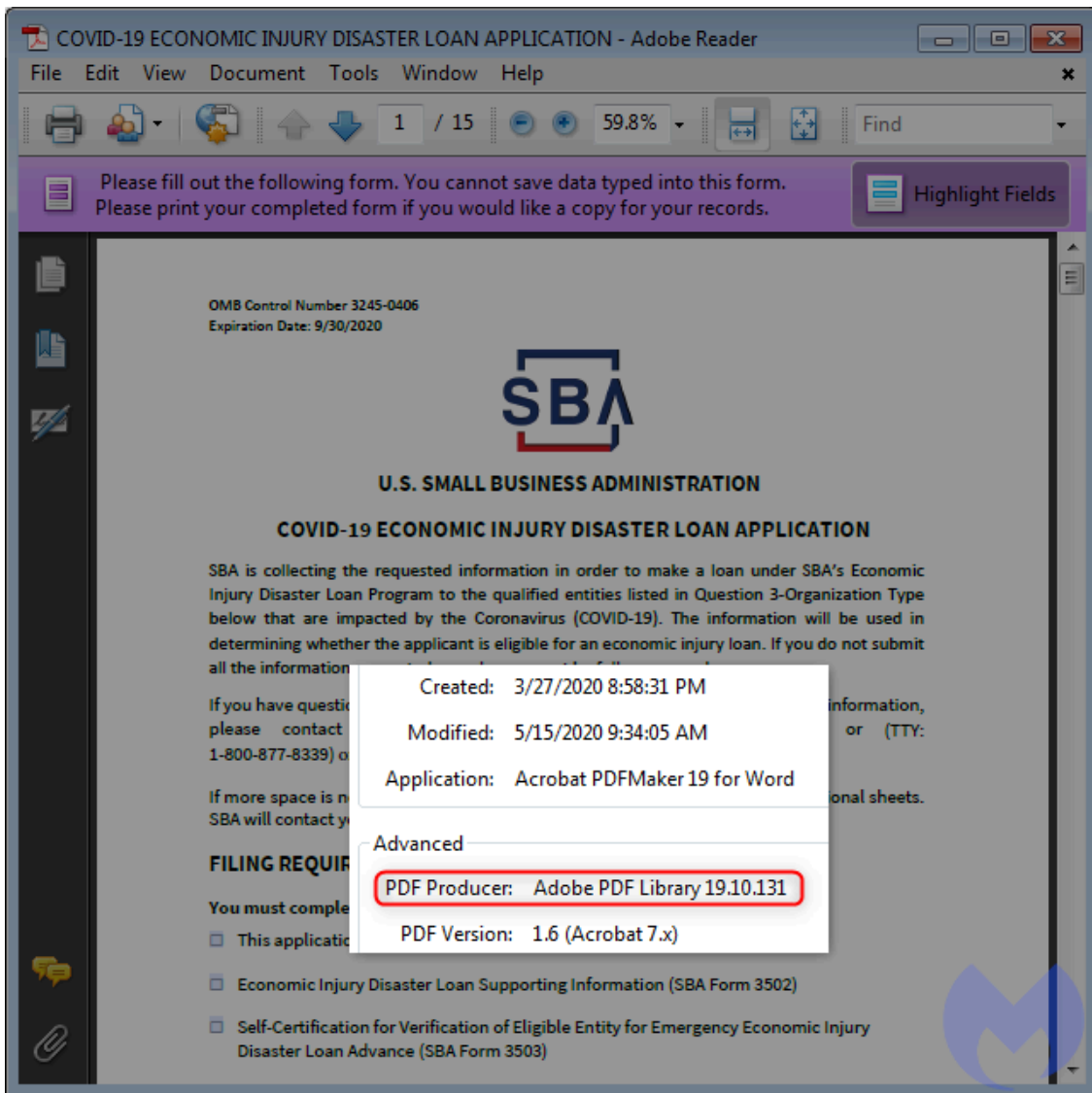
One of the items to look at is the “Received” field. In this case, it shows a hostname (park-mx.above[.]com) that looks suspicious. In fact, we can see it has already been mentioned in [another scam campaign](#).

If we go back to this email, we see that it contains an attachment, a loan application with the 3245-0406 reference number. A look at the PDF metadata can sometimes reveal interesting information.



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~  
Domain Name: gov-sba.us  
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF4235C-NSR  
Registrar WHOIS Server:  
Registrar URL: www.psi-usa.info  
Updated Date: 2020-08-05T06:22:13Z  
Creation Date: 2020-07-31T06:22:09Z  
Registry Expiry Date: 2021-07-31T06:22:09Z  
Registrar: PSI-USA, Inc. dba Domain Robot  
Registrar IANA ID: 151  
Registrar Abuse Contact Email:  
Registrar Abuse Contact Phone:  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr  
ansferProhibited  
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR  
Registrant Name: Krikor Derabrahamian  
Registrant Organization:  
Registrant Street: Rotenloewengasse 15  
Registrant Street:  
Registrant Street:  
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

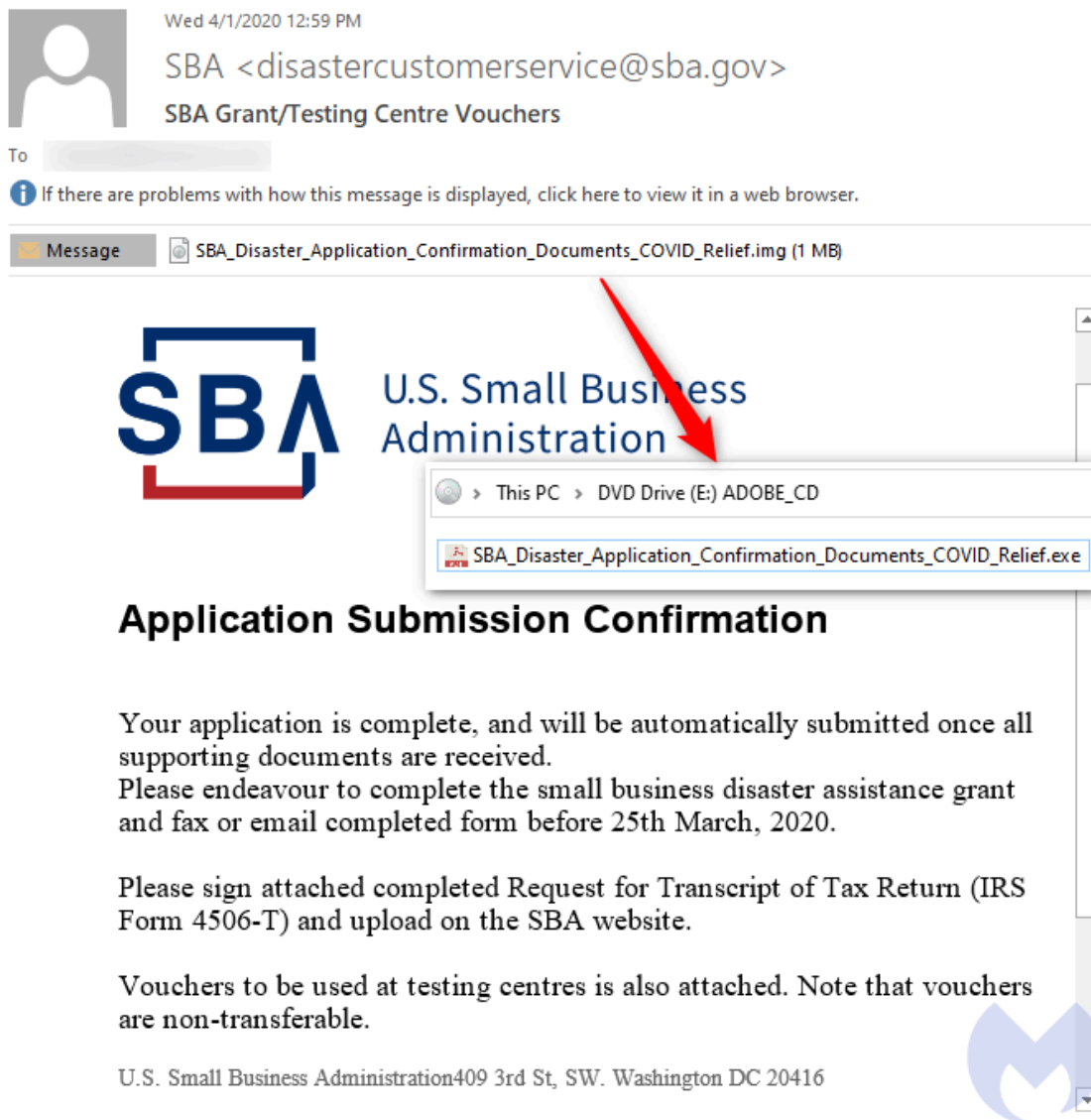
There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to phishing emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

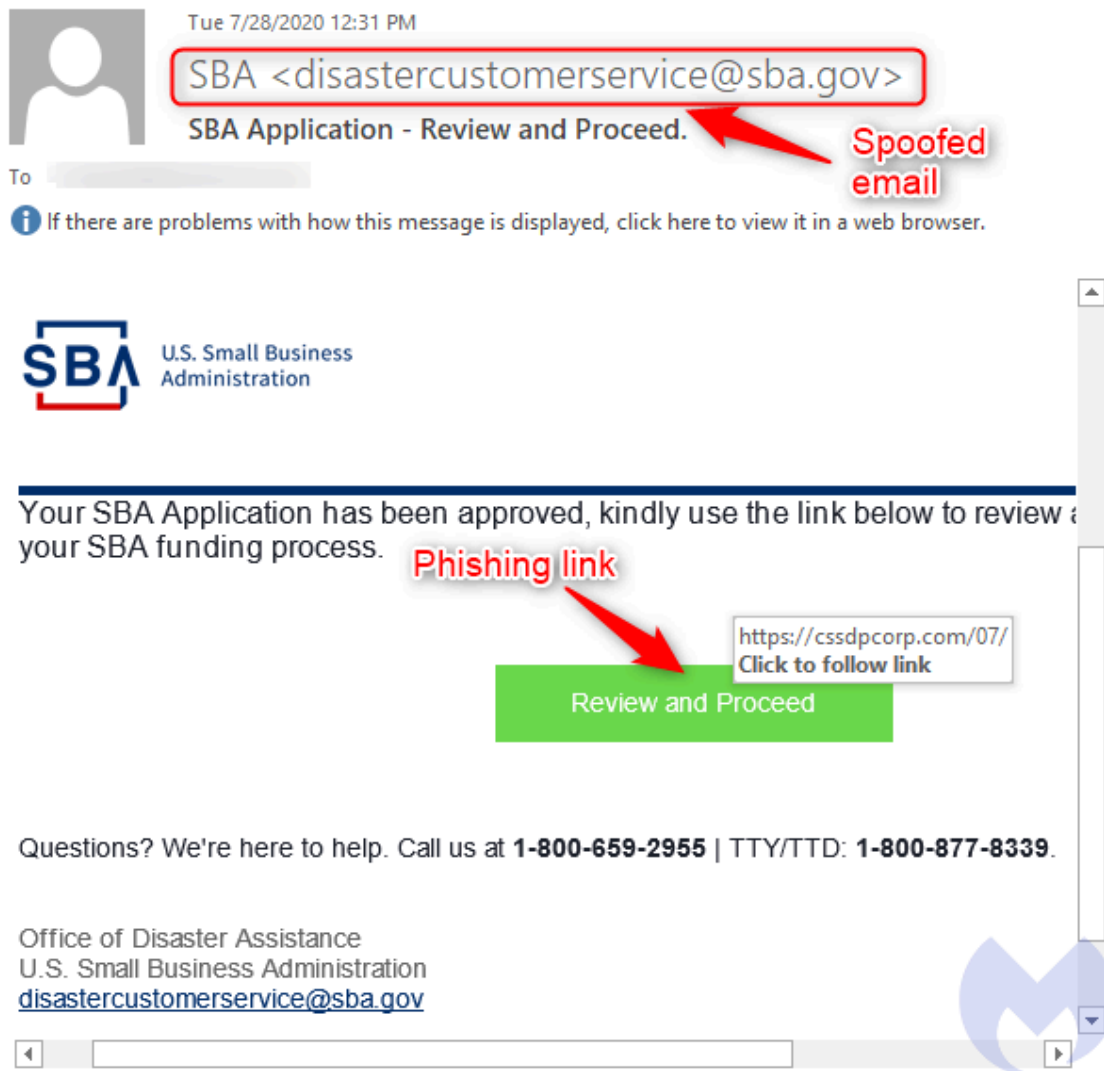
[Malwarebytes](#) also protects against phishing attacks and malware by blocking offending infrastructure used by scammers.



The malware was the popular [GuLoader](#), a stealthy downloader used by criminals to load the payload of their choice and bypass antivirus detection.

Traditional phishing attempt

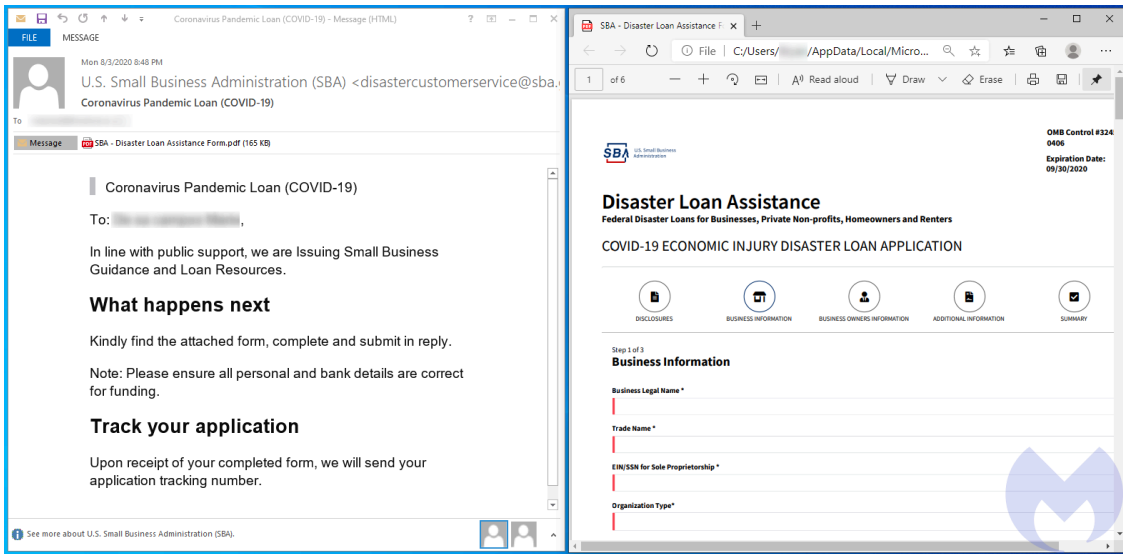
The second wave we saw involved a more traditional phishing approach where the goal was to collect credentials from victims in order to scam them later on.



A URL, especially if it has nothing to do with the sender, is a big giveaway that the email may be fraudulent. But things get a little more complicated when attackers are using attachments that look seemingly legitimate.

Advanced phishing attempt

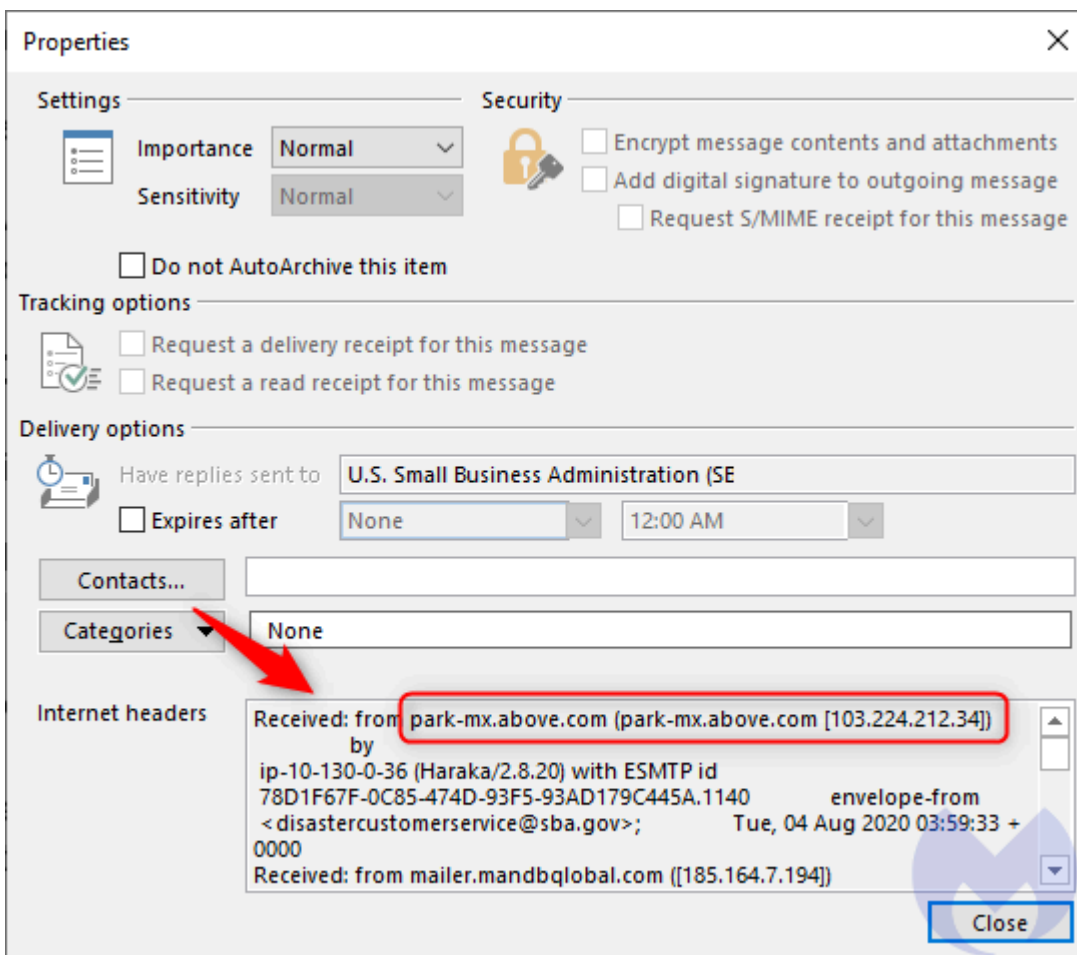
This is what we saw in a pretty clever and daring scheme that tricks people into completing a full form containing highly personal information, including bank account details. These could be used to directly drain accounts or in an additional layer of social engineering, which tricks users into paying in advanced fees that don't exist as part of the real SBA program.



This latest campaign started in early August and is convincing enough to fool even seasoned security experts. Here’s a closer look at some red flags we encountered as we analyzed it.

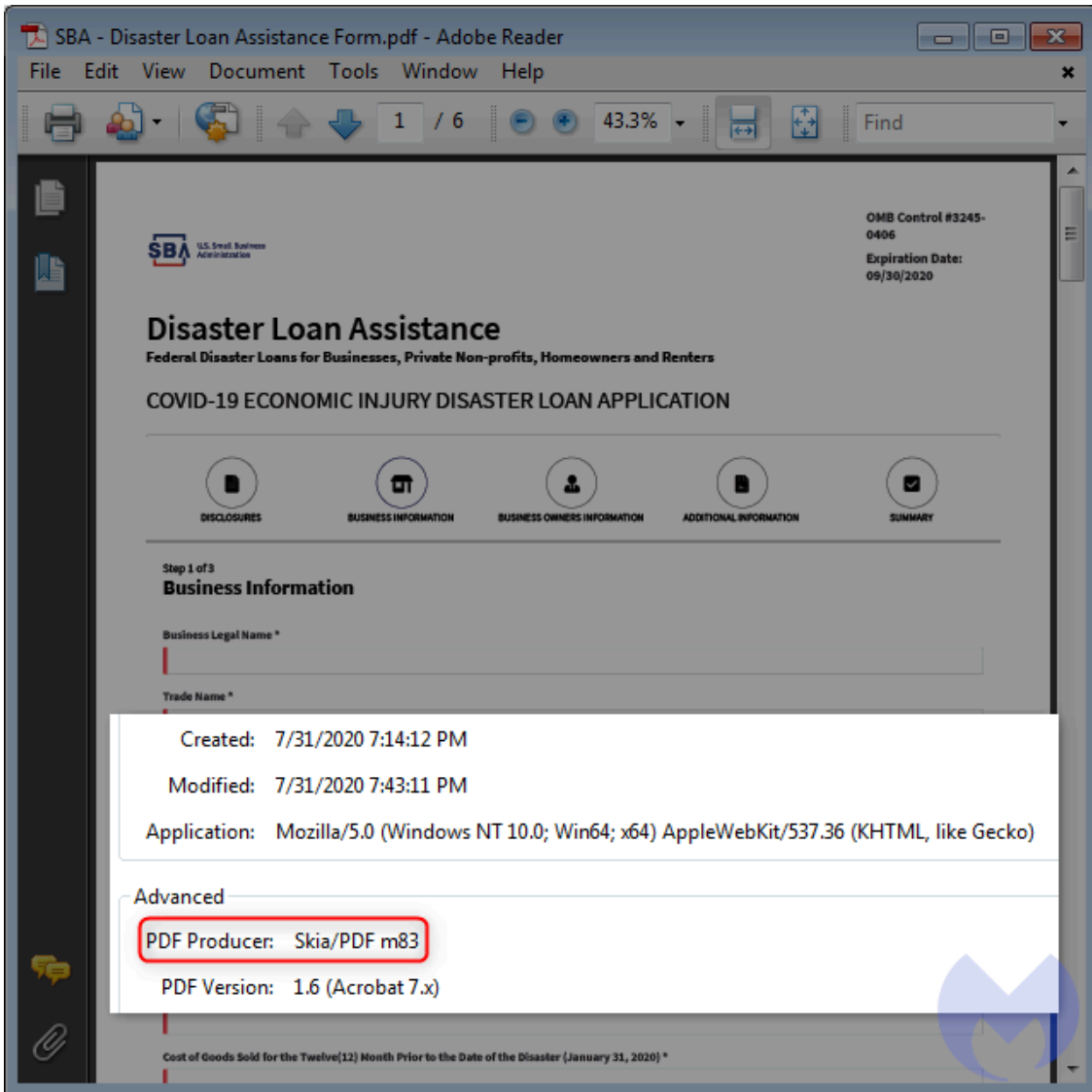
Most people aren’t aware of [email spoofing](#) and believe that if the sender’s email matches that of a legitimate organization, it must be real. Unfortunately, that is not the case, and there are additional checks that need to be performed to confirm the authenticity of a sender.

There are various technologies for confirming the true sender email address, but we will instead focus on the emails headers, a sort of blue print that is available to anyone. Depending on the email client, there are different ways to view such headers. In Outlook, you can click File and then Properties to display them:



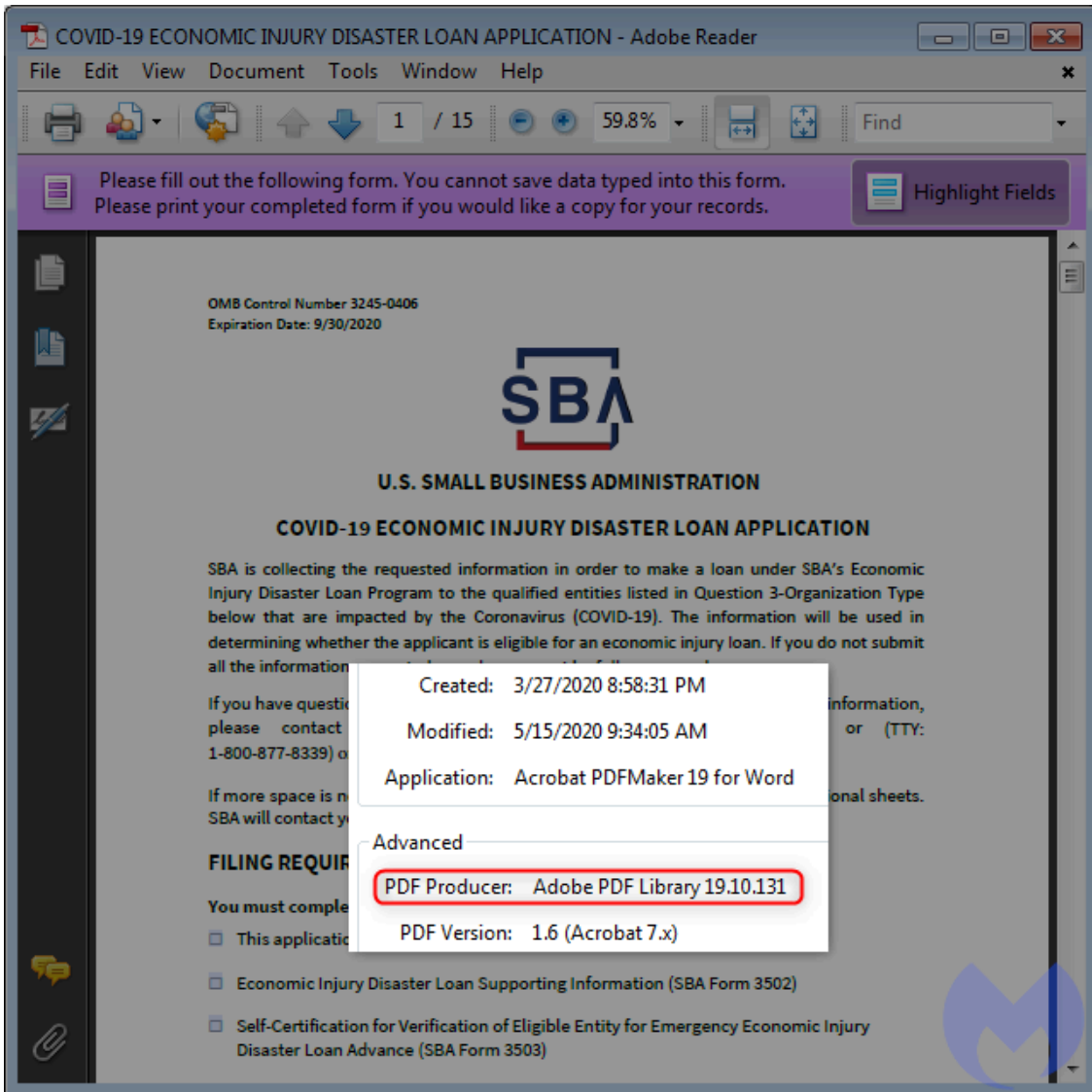
One of the items to look at is the “Received” field. In this case, it shows a hostname (park-mx.above[.]com) that looks suspicious. In fact, we can see it has already been mentioned in [another scam campaign](#).

If we go back to this email, we see that it contains an attachment, a loan application with the 3245-0406 reference number. A look at the PDF metadata can sometimes reveal interesting information.



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~
Domain Name: gov-sba.us
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF4235C-NSR
Registrar WHOIS Server:
Registrar URL: www.psi-usa.info
Updated Date: 2020-08-05T06:22:13Z
Creation Date: 2020-07-31T06:22:09Z
Registry Expiry Date: 2021-07-31T06:22:09Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr
ansferProhibited
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR
Registrant Name: Krikor Derabrahamian
Registrant Organization:
Registrant Street: Rotenloewengasse 15
Registrant Street:
Registrant Street:
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to phishing emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

[Malwarebytes](#) also protects against phishing attacks and malware by blocking offending infrastructure used by scammers.

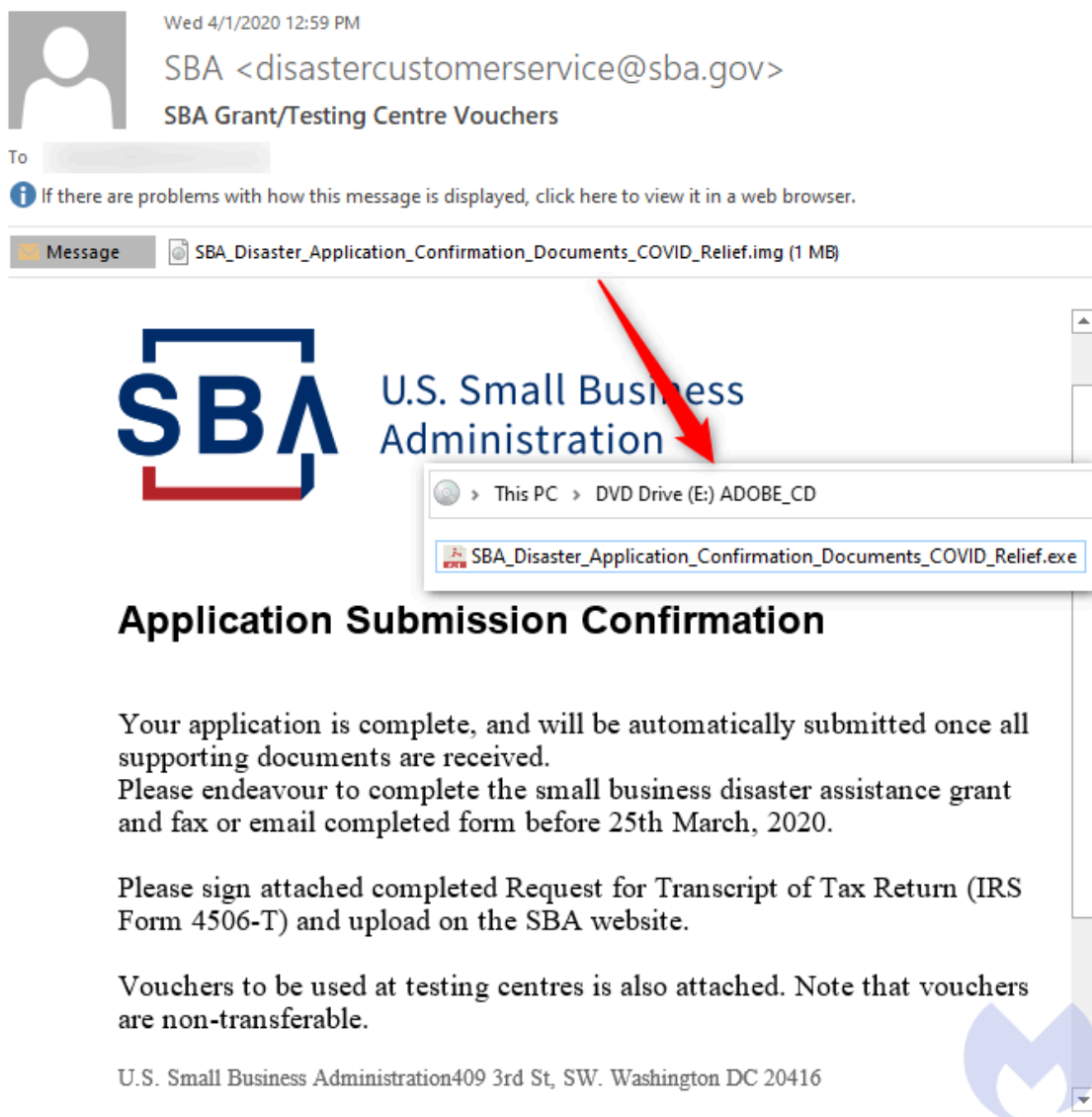
A number of threat actors continue to take advantage of the ongoing coronavirus pandemic through phishing scams and other campaigns distributing malware.

In this blog, we look at 3 different phishing waves targeting applicants for Covid-19 relief loans. The phishing emails impersonate the US Small Business Administration (SBA), and are aimed at delivering malware, stealing user credentials or committing financial fraud.

In each of these campaigns, criminals are spoofing the sender's email so that it looks like the official SBA's. This technique is very common and unfortunately often misunderstood, resulting in many successful scams.

GuLoader malware

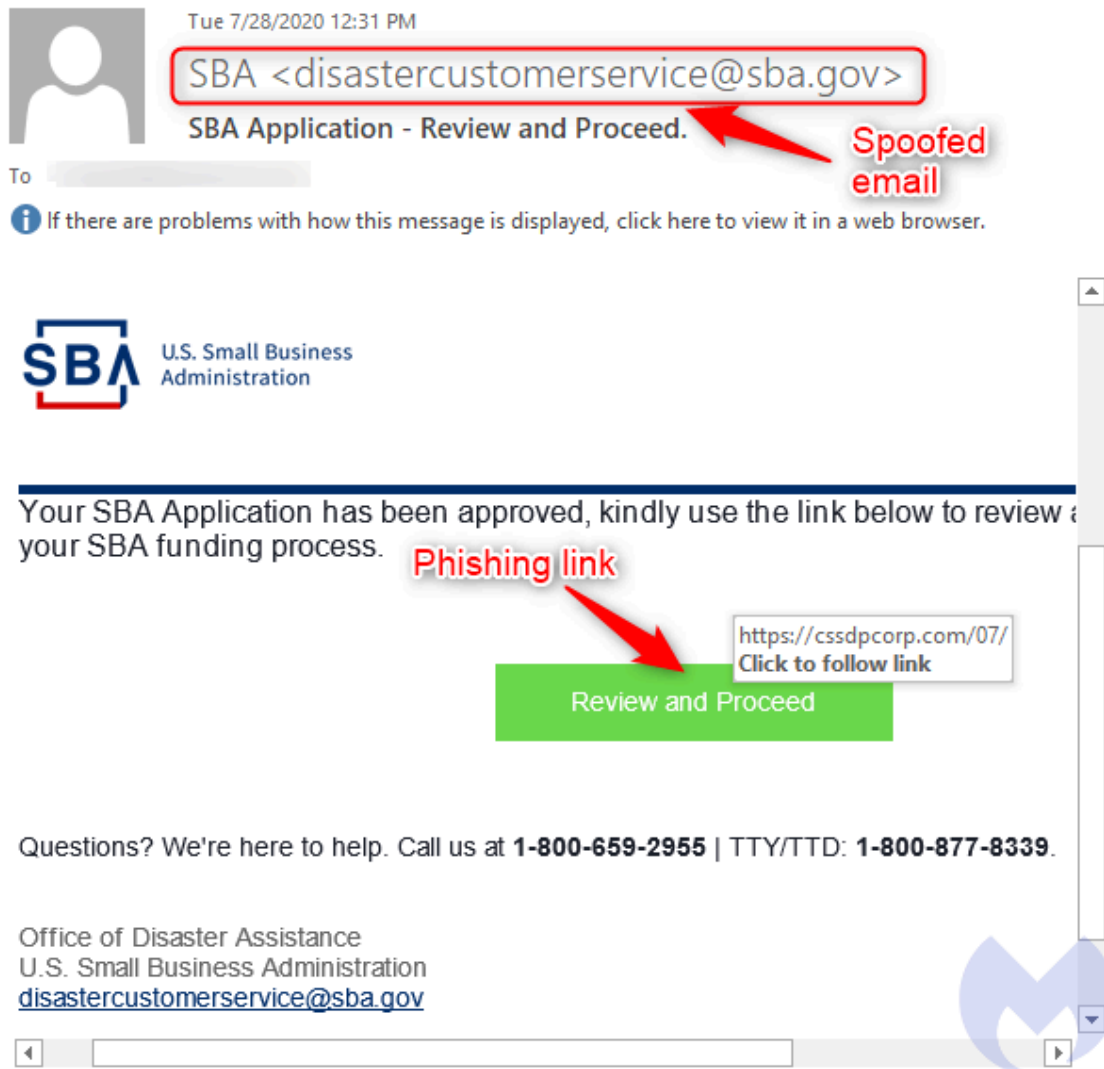
In April, we saw the first wave of SBA attacks using COVID-19 as a lure to distribute malware. The emails contained attachments with names such as 'SBA_Disaster_Application_Confirmation_Documents_COVID_Relief.img'.



The malware was the popular [GuLoader](#), a stealthy downloader used by criminals to load the payload of their choice and bypass antivirus detection.

Traditional phishing attempt

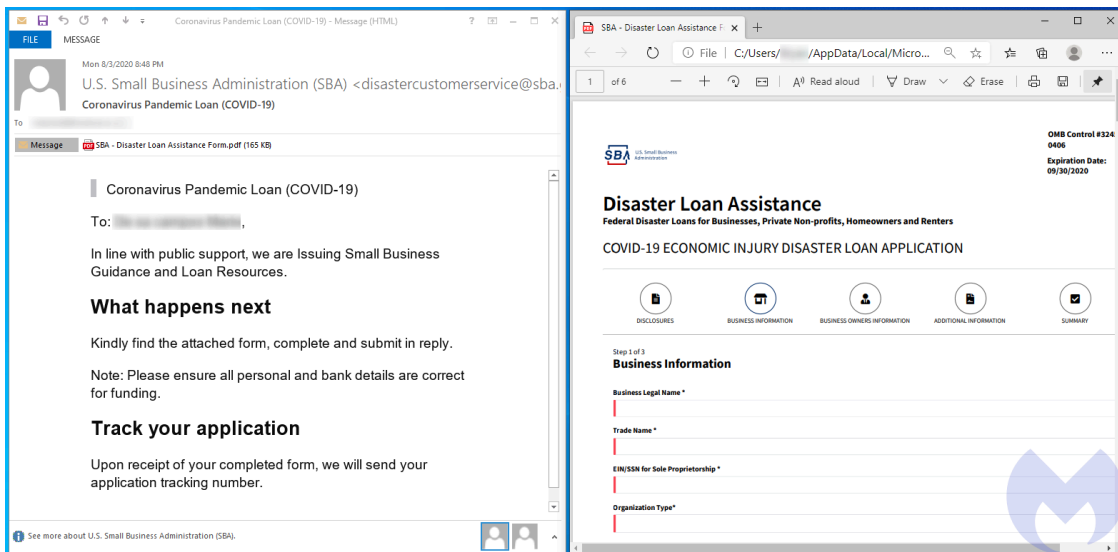
The second wave we saw involved a more traditional phishing approach where the goal was to collect credentials from victims in order to scam them later on.



A URL, especially if it has nothing to do with the sender, is a big giveaway that the email may be fraudulent. But things get a little more complicated when attackers are using attachments that look seemingly legitimate.

Advanced phishing attempt

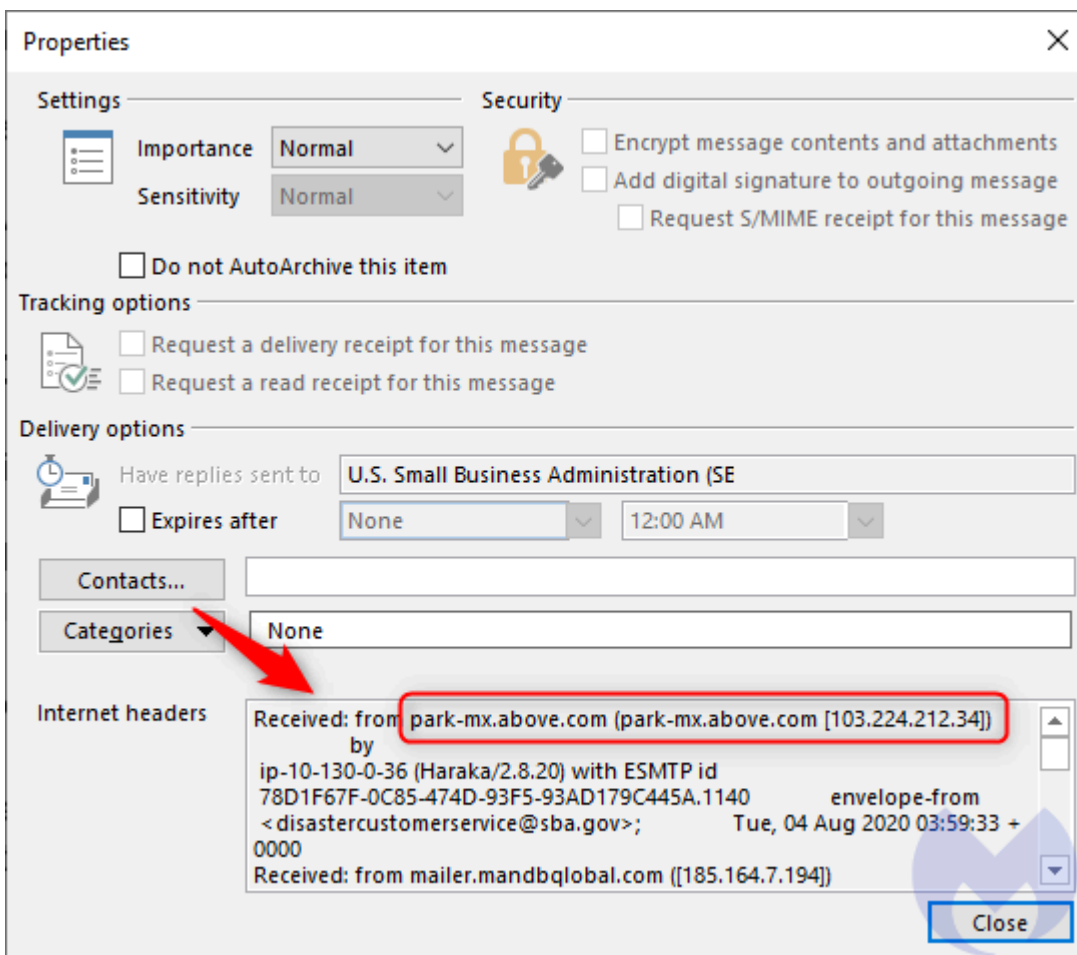
This is what we saw in a pretty clever and daring scheme that tricks people into completing a full form containing highly personal information, including bank account details. These could be used to directly drain accounts or in an additional layer of social engineering, which tricks users into paying in advanced fees that don't exist as part of the real SBA program.



This latest campaign started in early August and is convincing enough to fool even seasoned security experts. Here's a closer look at some red flags we encountered as we analyzed it.

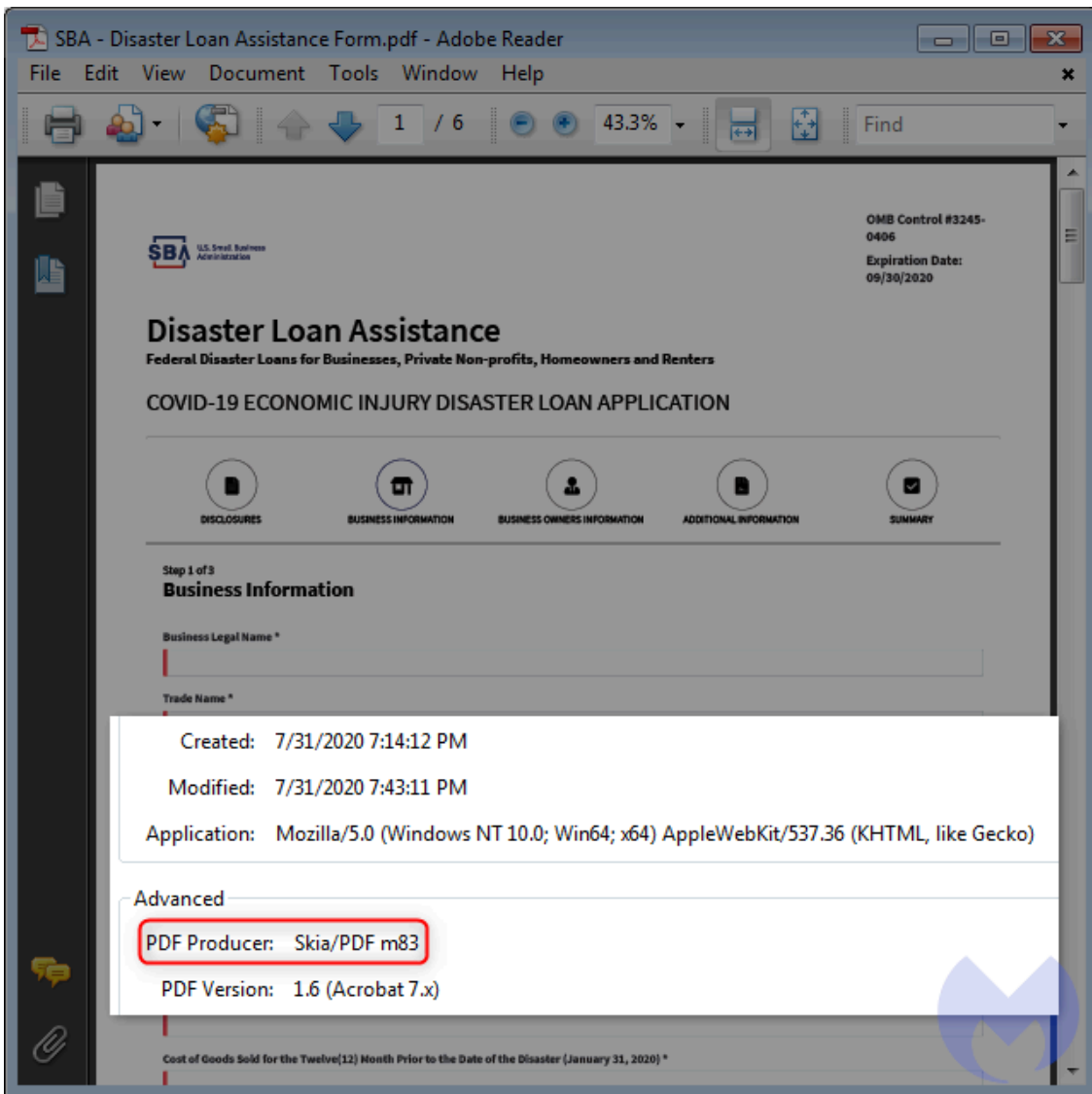
Most people aren't aware of [email spoofing](#) and believe that if the sender's email matches that of a legitimate organization, it must be real. Unfortunately, that is not the case, and there are additional checks that need to be performed to confirm the authenticity of a sender.

There are various technologies for confirming the true sender email address, but we will instead focus on the emails headers, a sort of blue print that is available to anyone. Depending on the email client, there are different ways to view such headers. In Outlook, you can click File and then Properties to display them:



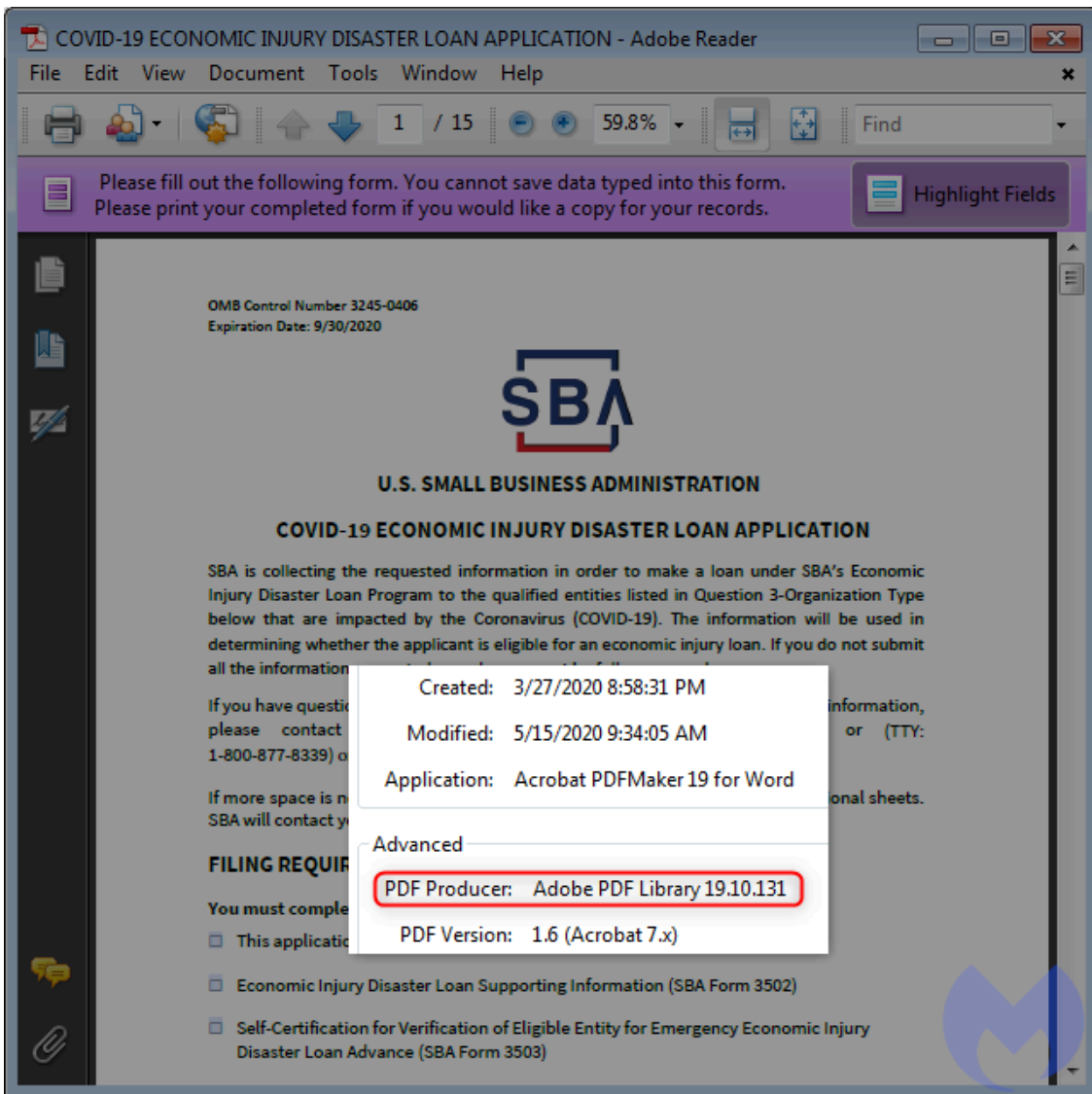
One of the items to look at is the “Received” field. In this case, it shows a hostname (park-mx.above[.]com) that looks suspicious. In fact, we can see it has already been mentioned in [another scam campaign](#).

If we go back to this email, we see that it contains an attachment, a loan application with the 3245-0406 reference number. A look at the PDF metadata can sometimes reveal interesting information.



Here we note the file was created on July 31 with Skia, a graphics library for Chrome. This tells us that the fraudsters created that form shortly before sending the spam emails.

For comparison, if we look at the application downloaded from the official SBA website, we see some different metadata:



This legitimate application form was created used Acrobat PDFMaker for Word on March 27 which coincides with the pandemic timeline.

The loan application would typically be printed out and then mailed to a physical address at one of the government offices. If we go back to the original email, it asks to send the completed form as a reply via email instead:

This is where things get interesting. Even though the sender's email is disastercustomerservice@sba.gov, when you hit the reply button, it shows a different email address at: [disastercustomerservice@gov-sba\[.\]us](mailto:disastercustomerservice@gov-sba[.]us). While sba.gov is the official and legitimate government website, [gov-sba\[.\]us](http://gov-sba[.]us) is not.

```
user@user: ~  
Domain Name: gov-sba.us  
Registry Domain ID: D18007599F1554B3DAA9B6AFEAF4235C-NSR  
Registrar WHOIS Server:  
Registrar URL: www.psi-usa.info  
Updated Date: 2020-08-05T06:22:13Z  
Creation Date: 2020-07-31T06:22:09Z  
Registry Expiry Date: 2021-07-31T06:22:09Z  
Registrar: PSI-USA, Inc. dba Domain Robot  
Registrar IANA ID: 151  
Registrar Abuse Contact Email:  
Registrar Abuse Contact Phone:  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTr  
ansferProhibited  
Registry Registrant ID: C186298DF566447488A165F7E4F5B8F60-NSR  
Registrant Name: Krikor Derabrahamian  
Registrant Organization:  
Registrant Street: Rotenloewengasse 15  
Registrant Street:  
Registrant Street:  
Registrant City: Wien
```

That domain name (gov-sba[.]us) was registered just days before the email campaign began and clearly does not belong to the US government.

However, we should note that this campaign is quite elaborate and that it would be easy to fall for it. Sadly, the last thing you would want when applying for a loan is to be out of even more money.

If you reply to this email with the completed form containing private information that includes your bank account details, this is exactly what would happen.

Tips on how to protect yourself

There is no question that people should be extremely cautious whenever they are asked to fill out information online—especially in an email. Fraudsters are lurking at every corner and ready to pounce on the next opportunity.

Both the [Department of Justice](#) and the [Small Business Administration](#) have been warning of scams pertaining to SBA loans. Their respective sites provide various tips on how to steer clear of various malicious schemes.

Perhaps the biggest takeaway, especially when it comes to phishing emails, is that the sender’s address can easily be spoofed and is in no way a solid guarantee of legitimacy, even if it looks exactly the same.

Because we can’t expect everyone to be checking for email headers and metadata, at least we can suggest double checking the legitimacy of any communication with a friend or by phoning the government organization. For the latter we always recommend to never dial the number found in an email or left on a voicemail, as it could be fake. Google the organization for its correct contact number.

[Malwarebytes](#) also protects against phishing attacks and malware by blocking offending infrastructure used by scammers.

Source: <https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/>