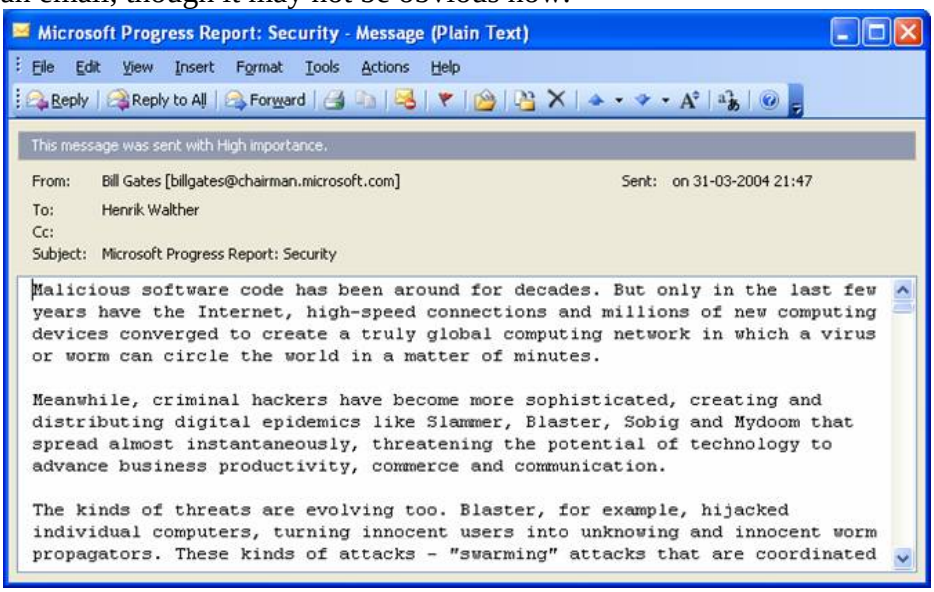
Email Expanded Header: Viewing in Microsoft Outlook

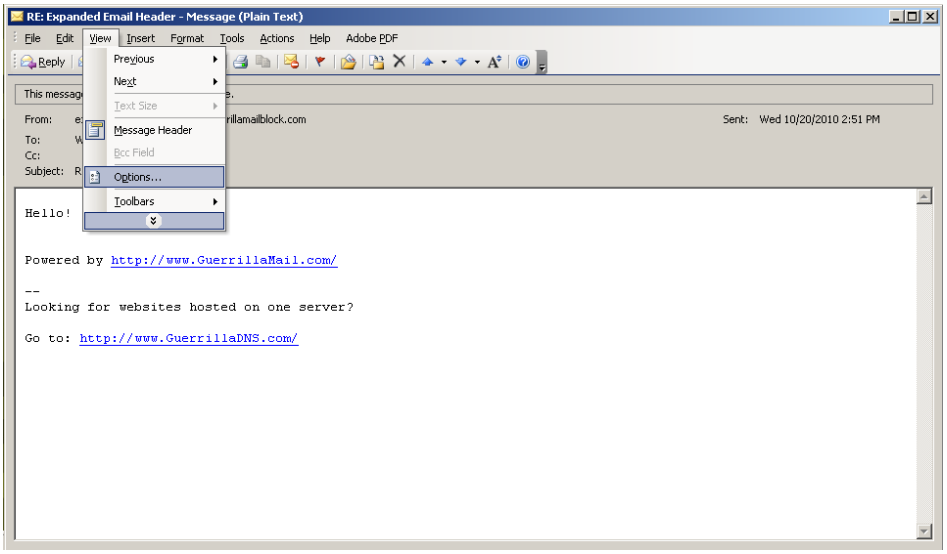
Figure 1: Default Shown Header in an Outlook 2003 E-mail Message

The Internet header of an e-mail message can have twenty lines or more showing all kinds of information about the message, like which servers the email has traveled through and when. Your e-mail program can also display the "full" header of an email, though it may not be obvious how.

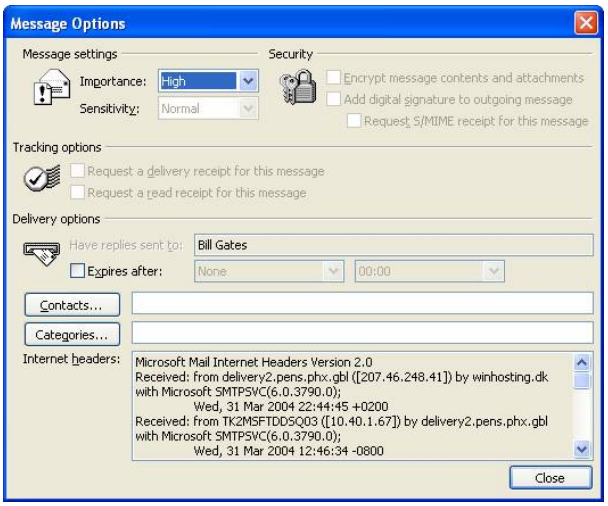


View Email Headers in Outlook 2003

- On **Options** under the **View** tab



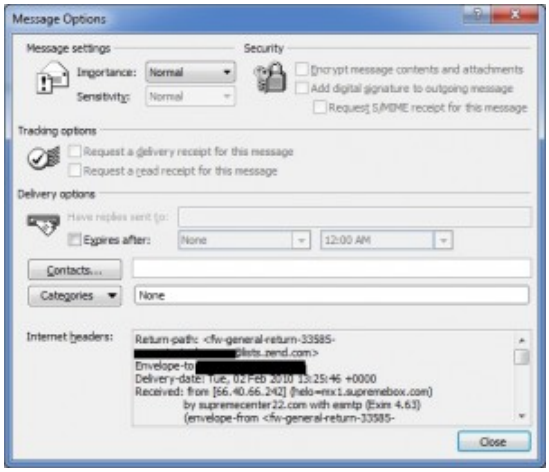
- Internet headed can be copied out of the **Internet headers** block into an email.



View Email Headers in Outlook 2007

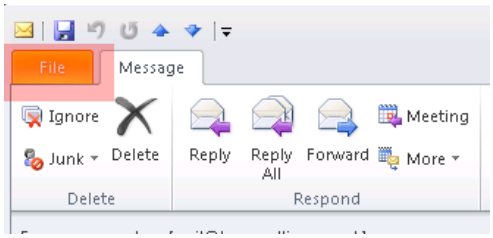
- On the **Options** section on the **Message** ribbon.

- Click the extender button to show Message Options

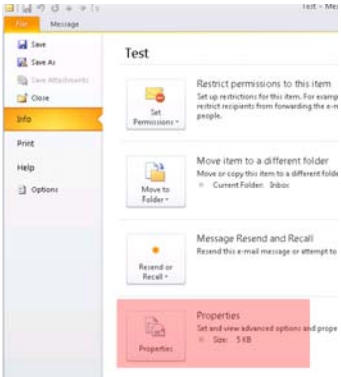


View Email Headers in Outlook 2010

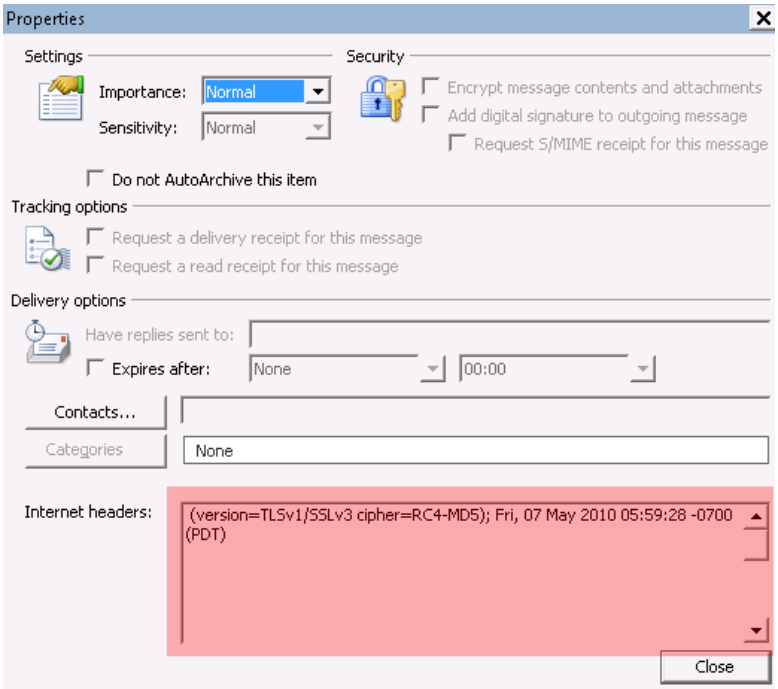
- Open the email you wish to view the headers for. Then click the **File** menu.



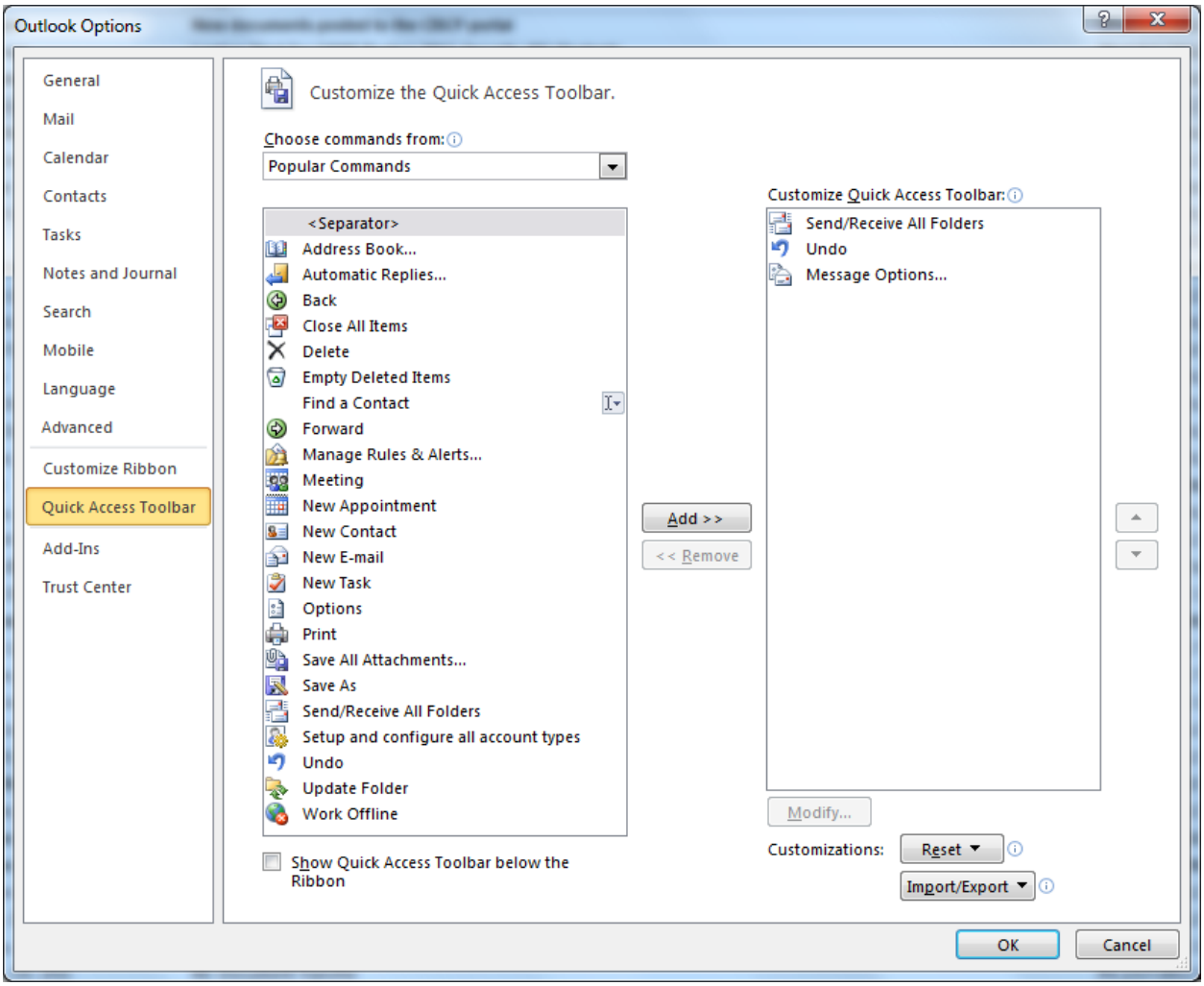
- Click the **Properties** button in the menu



- A new window will open and it will show you the headers



To view email headers in Outlook 2010 without opening the email message, go to File → Options then select the “Quick Access Toolbar”. Choose “Message Options…” and click “Add > >” to add it to the Customize Quick Access Toolbar menu. Click OK.



To view the message header, you only need to select the email message and then click the “Message Options…” symbol in the top left corner to reveal the header.

Understanding Email Header Information

```
Return-Path: xx.com
Received: from imta11.westchester.pa.mail.comcast.net (LHLO
IMTA11.westchester.pa.mail.comcast.net) (76.96.62.22) by
sz0152.wc.mail.comcast.net with LMTP; Sun, 3 May 2009 07:32:03 +0000 (UTC)
Received: from web35402.mail.mud.yahoo.com ([66.163.179.111])
by IMTA11.westchester.pa.mail.comcast.net with comcast
id mvY31b00a2Qc7hu0BvY3Le; Sun, 03 May 2009 07:32:03 +0000
X-Authority-Analysis: v=1.0 c=1 a=OOqQ1alfmMHBQ5mv+1ZDpg==:17
a=C_IRinGWAAAA:8 a=CjxXgO3LAAAA:8 a=LtGpxU-LAAAA:8 a=1XWaLZrsAAAA:8
a=cVjbZSJ2AAAA:8 a=4wmYmKVIaK1lp7vLyp8A:9
a=kwv9yk7nxi8NNw45YxmOQevxPUsA:4
a=aQrGmxF-vzIA:10 a=si9q_4b84H0A:10 a=rC2wZJ5BpNYA:10 a=eL4mtSqiQiEA:10
Received: (qmail 95160 invoked by uid 60001); 3 May 2009 07:32:02 -0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s1024;
t=1241335922; bh=TgdYnYlQ5kFiTJeXh0JZqRtFp+hfAMX+vqhOndQhnpc=;
h=Message-ID:X-YMail-OSG:Received:X-Mailer:Date:From:Subject:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
b=CITTfK1I2RlgV3vOD24JvOCijQZ6irLNFC/c6/1xAg264J1tgoKzIYVUtc6flCBeYGqMVLg
0+rFMlqPpMrQbTIQeJ6WupROus54mphGm/w+xJR/w+dxn4VHDf3Rh8NG9CB/vfDzZQ
zUkp1GppoyVV+KR5SP/J/0x3C0GfjwL35U=
DomainKey-Signature:a=rsa-sha1; q=dns; c=nofws;
s=s1024; d=yahoo.com;
h=Message-ID:X-YMail-OSG:Received:X-Mailer:Date:From:Subject:To:MIME-
Version:Content-Type:Content-Transfer-Encoding;
b=w7PzSiqxraRC96Q8S98gD34esNRRokuBH03S1pSAfUtCkaCGzIhJdL5QhcluwgD+/T
C+97BPhqr8lhni207SPV5EyFCIuhucPX6QzC/+sqkgNOlxibotx2GOmvPnzbfZuDb6+8T
GZ1e4Mnog6OqyDUaA1venhzno1se5nLJLAjM=;
Message-ID: <53270.94542.qm@web35402.mail.mud.yahoo.com>
X-YMail-OSG:
.V7RRvMVM1lstVihJQhVCL1gPOr2evd7MxzkLhufduHpCWVAfkbV.0AsPoBj0k78.TIn7oL
UGkHdCxzNta4iDpwzaUyNoM7BMoLqKJQi.aFYqZmXGI8fuxde7ftDAtm4nFcC6afPHWV
EvezHD1Y4H2SKZUrmg.VNDDK7SLpCrNM7Pi2qBe3WgjP5WZQTH2A1sB8W7b_K6ySR
76Oiq6upH40snO8PSy0sA3YIdb.5iVEpDxrrmUT133HZT5.xMFIraLLyRSQ1P.fhPRSFFux
SlftRb11BKgttvIO6U6e3dtEwWx5W5uOmfdm4Mba1P03FfA_ykyWPgr_G2FZKNneThi0
guuiQW7cznCYMoJ_bp50iLw--
Received: from [222.123.176.219] by web35402.mail.mud.yahoo.com via HTTP;
Sun, 03 May 2009 00:32:02 PDT
X-Mailer: YahooMailClassic/5.2.20 YahooMailWebService/0.7.289.1
Date: Sun, 3 May 2009 00:32:02 -0700 (PDT)
From: m s
Subject: Seek and Ye Shall Find
To: xx.net
MIME-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable
```

Key Notes:

- Email headers read **bottom to top**. The first IP address listed is the last person to receive the email.
- The last IP address in the header is the originator IP address.
- IP addresses are traceable. (This one is from Thailand.)
- Message-ID: is a unique identifier generated for this email.

Since the winter holidays are quickly approaching, US-CERT is republishing this entry to increase awareness about phishing scams and malware campaigns.

In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the winter holidays and holiday shopping season. Users who are new to making seasonal online purchases are encouraged to take care and use safe online shopping habits.

US-CERT reminds users to remain cautious when receiving unsolicited email messages that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include but are not limited to the following:

- Electronic greeting cards that may contain malware
- Requests for charitable contributions that may be phishing scams and may originate from illegitimate sources claiming to be charities
- Screensavers or other forms of media that may contain malware
- Credit card applications that may be phishing scams or identity theft attempts
- Online shopping advertisements that may be phishing scams or identity theft attempts from bogus retailers

US-CERT encourages users and administrators to use caution when encountering these types of email messages and take the following preventative measures to protect themselves from phishing scams and malware campaigns:

- Refer to the Shopping Safely Online <http://www.us-cert.gov/cas/tips/ST07-001.html> Cyber Security Tip for more information on online shopping safety.
- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the Using Caution with Email Attachments <http://www.us-cert.gov/cas/tips/ST04-010.html> Cyber Security Tip for more information on safely handling email attachments.
- Maintain up-to-date antivirus software.
- Review the Federal Trade Commission's Charity Checklist <http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel01.shtm>.
- Verify charity authenticity through a trusted contact number.
- Trusted contact information can be found on the Better Business Bureau's National Charity Report Index <http://charityreports.bbb.org/public/All.aspx?bureauID=9999>.
- Refer to the Recognizing and Avoiding Email Scams <http://www.us-cert.gov/reading_room/emailscams_0905.pdf> (pdf) document for more information on avoiding email scams.
  Refer to the Avoiding Social Engineering and Phishing Attacks <http://www.us-cert.gov/cas/tips/ST04-014.html> Cyber Security Tip for more information on social engineering attacks.

Internet Crime Complaint Center

Data, Tools, and Resources for Enforcement Professionals

The Internet Crime Complaint Center (IC3) is an alliance between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). IC3's mission is to address crime committed over the Internet. For victims of Internet crime, IC3 provides a convenient and easy way to alert authorities of a suspected violation. For law enforcement and regulatory agencies, IC3 offers a central repository for complaints related to Internet crime, uses the information to quantify patterns, and provides timely statistical data of current trends.

Features

- Provides a central point for Internet crime victims to report and to alert an appropriate agency on-line at **www.ic3.gov**
- Collects, reviews, and refers Internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts
- Identifies current crime trends over the Internet

Benefits

- Provides an analytical repository for Internet crime complaints
- Analyzes and refers all fraudulent activity identified on the Internet to the appropriate local, state, or federal law enforcement authority
- Aids in the development of law enforcement training to address identified Internet crime problems
- Serves as the catalyst that allows law enforcement and regulatory agencies to network and share data
- Potentially reduces the amount of economic loss by Internet crime throughout the United States

To file an Internet crime complaint, visit the IC3 Web site at www.ic3.gov.

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

August 2005

DSS Malware Submission Guidelines

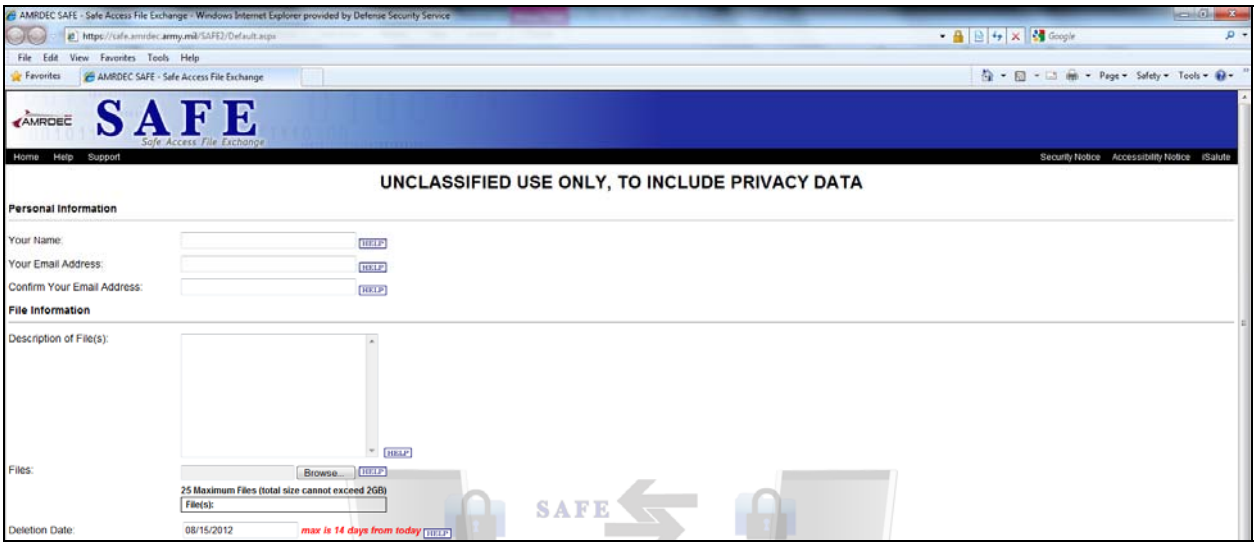
(Updated August 1, 2012)

Please use the following procedures to submit your suspicious file. You may choose one of the following two options:

OPTION 1

1. In order to prevent inadvertent compromises of the Department of Defense network, confirmed or suspected malicious files must be handled in a manner that minimizes the risk of damage to the network. As such, DSS is now utilizing a trusted, secure file transfer service to receive all suspect files for analysis.

2. All files requiring analysis will now be uploaded directly from the CDC to https://safe.amrdec.army.mil/SAFE2/Default.aspx. From within this web portal, the requestor will enter their personal information, upload the file and a brief description and enter the recipient information (dsscyberci@dss.mil). Detailed instructions are outlined below.



Personal Information

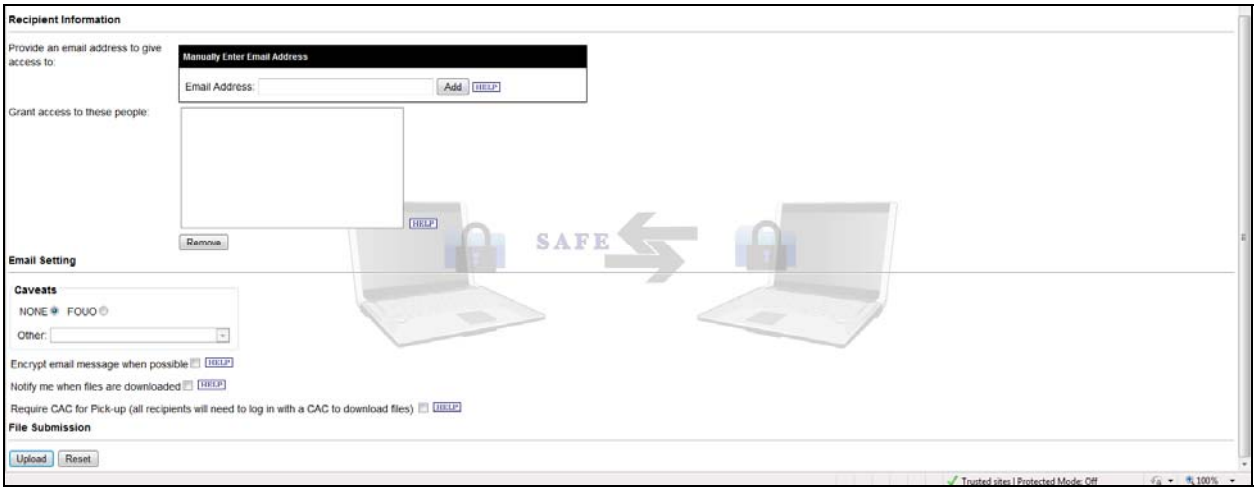
1. Enter Your Name (Person actually submitting the sample)
2. Enter Your Email Address (Person actually submitting the sample)
3. Confirm Your Email Address (Person actually submitting the sample)

File Information

1. Description of File(s): Enter the file name and the DSS local tracking number associated with it. If no DSS local tracking number is available, provide as much identifying information as possible (e.g. Facility/Company name submitting the file, CAGE code, DSS POC information, etc.)

2. Click “Browse…” to select and upload your file. Please note: As an additional security measure, this system is designed to strip out any malicious files uploaded to it. In order to prevent this and successfully upload your file, it **must** be placed in a password protected zipped file. Detailed instructions to do this are included below.

3. Deletion Date: Leave this as the default date.



Recipient Information

1. Provide an email address to give access to: Enter dsscyberci@dss.mil in this box and click “Add”. This will add it to the block below titled “Grant access to these people.”

Email Setting

1. Caveats. Please mark “FOUO”

2. Check “Encrypt email message when possible”

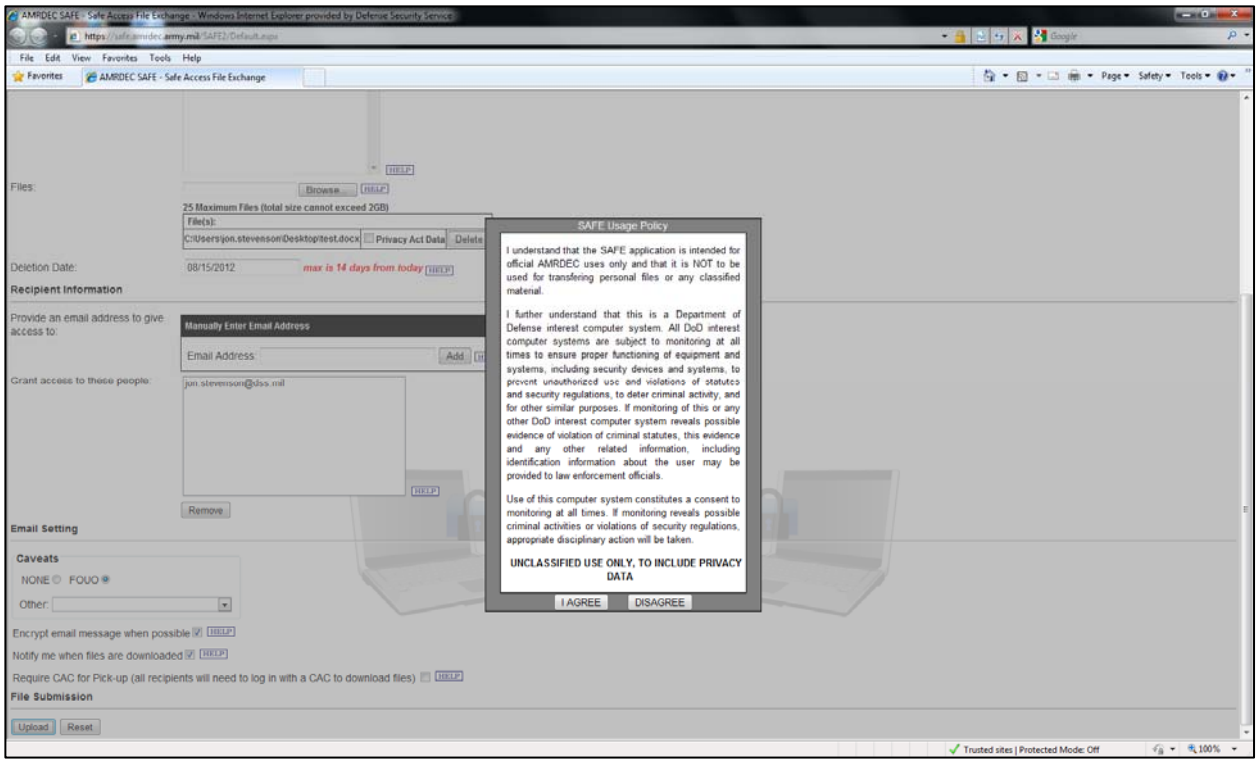
3. Choose whether or not you want to be notified when files are downloaded.

4. Do **NOT** check “Require CAC for Pick-up”

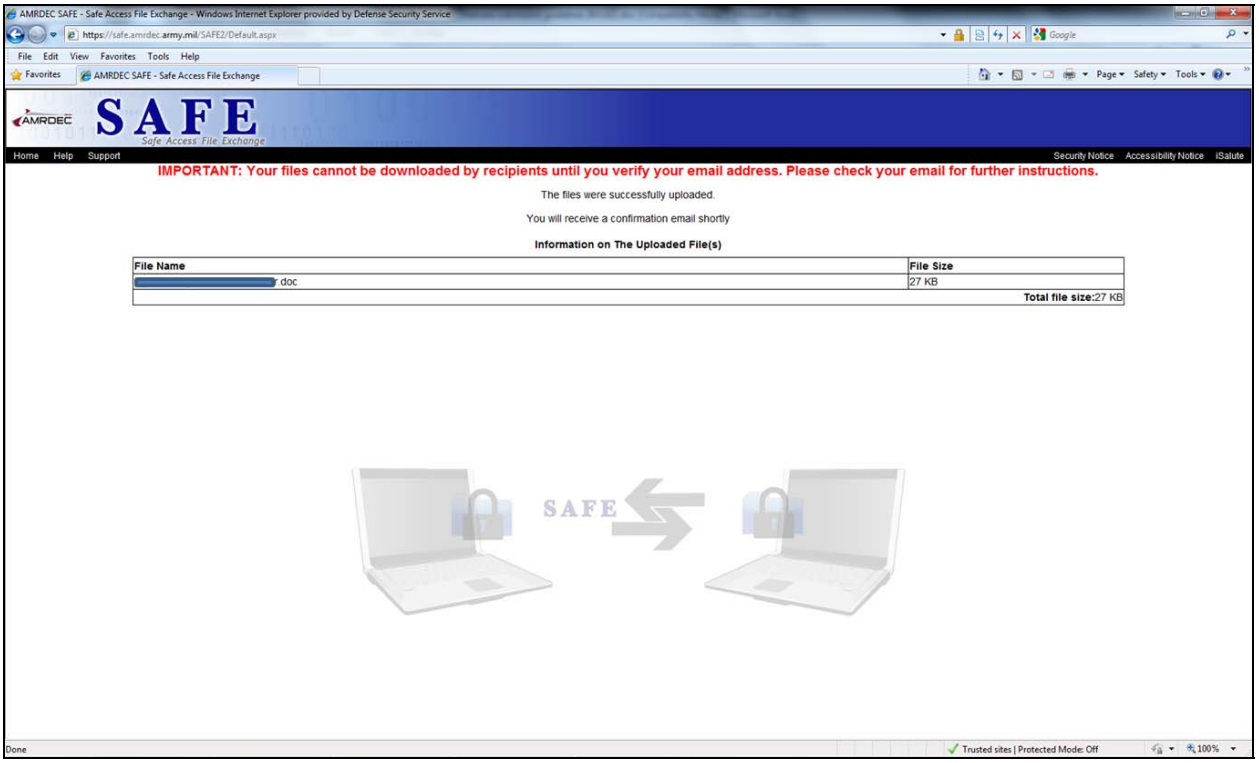
File Submission

1. If finished, click “Upload”

2. You will then see a “SAFE Usage Policy Window”. Click “I AGREE”.



3. You should then see a verification message that your file has been uploaded successfully.



Once uploaded, you will receive a verification email. Your file has not yet been submitted. You must click on the link in the email, enter the password provided and then click “Verify” to submit your file.

VERIFICATION IS REQUIRED - AMRDEC Safe Access File Exchange Submittal Notice - VERIFICATION IS REQUIRED - Message (Plain Text)

Subject: VERIFICATION IS REQUIRED - AMRDEC Safe Access File Exchange Submittal Notice - VERIFICATION IS REQUIRED

-----Original Message-----
From: WEBTeam@amrdec.army.mil [mailto:WEBTeam@amrdec.army.mil]
Sent: Tuesday, October 25, 2011 10:08 AM
To: [Recipient]
Subject: VERIFICATION IS REQUIRED - AMRDEC Safe Access File Exchange Submittal Notice - VERIFICATION IS REQUIRED
Importance: High

DO NOT FORWARD

AMRDEC Safe Access File Exchange Submittal Notice

Your Package has not yet been sent.
You MUST verify your email address in order for your recipients to download the file(s). Please use the link below to login and verifiy that you are the sender of this package.
https://safe.amrdec.army.mil/safe2/StatusLogIn.aspx?PackageID=[number] (AMRDEC SAFE)

If you did not send these files, please notify WebTeam@amrdec.army.mil ASAP.

You have uploaded the following file(s): Sample test file for transfer

Package ID:[number]

The file will be available until [Date]

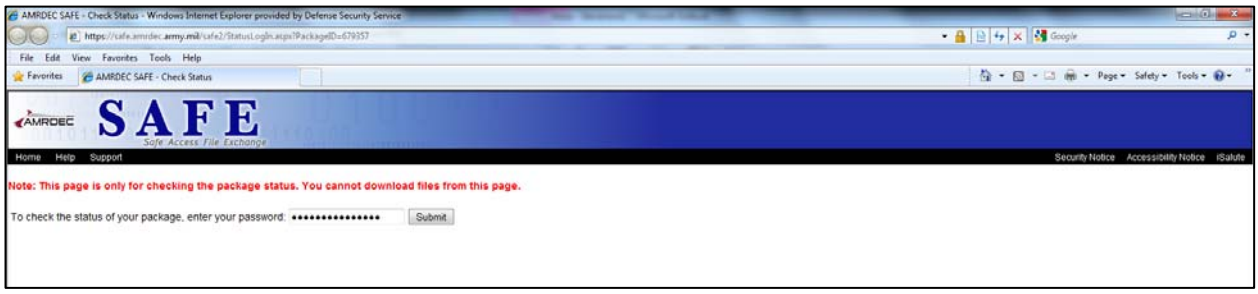
You can check the status of the files uploaded at https://safe.amrdec.army.mil/safe2/StatusLogIn.aspx?PackageID=[number] (AMRDEC SAFE)

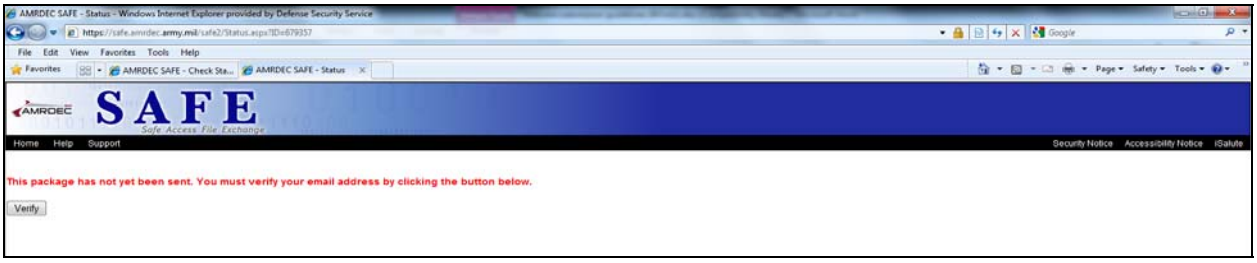
The Password is: xxxxxxxxxxxxxxxxx

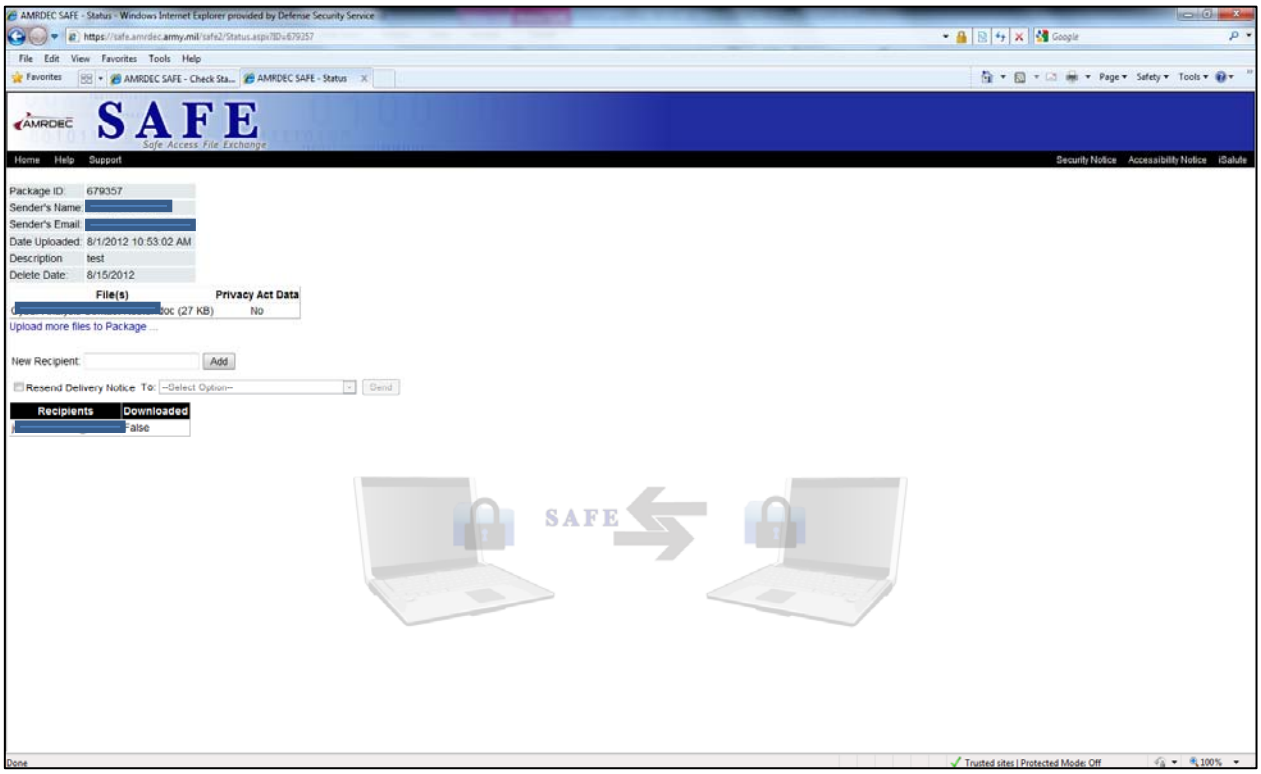
NOTICE: This e-mail message is intended solely for the use of the addressee. If the reader of this message is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately.

Thank you.

This message may be forwarded to webteam@amrdec.army.mil for technical support purposes.







OPTION 2

If the media is on a CD or DVD, it may be mailed to the following address:

Defense Security Service
Counterintelligence Directorate
ATTN: Cyber Analysis
27130 Telegraph Road
Quantico, VA 22134

Please call DSS Headquarters cyber analysts if you have questions or concerns. If you have any special circumstances outside of those covered above, please contact us to determine the best course of action. Also, if you have a very large file to submit (larger than 2 GB), please coordinate with a cyber analyst before you submit.

Preparing the files

1. If an SCR number has not been assigned, please have the CDC use your local tracking number for the incident number *(Example: FB-10-0233)*. Otherwise, please use the SCR number.

2. Place the malware in a zip file named as the incident number and the words "media submission." (Detailed procedures below)

Example: Submission of malware for incident FB-10-0233 would have a zip file named "FB-10-0233 MediaSubmission.zip"

Note: It is also acceptable to place a copy of the actual suspicious email (.msg file) in the zipped malware folder. This allows the original header data to easily be extracted from the email

3. If you have supporting data (e.g., log files, registry files, etc.) that is not malware but may aid in the analysis, place that in a zip file (no password) named for the incident number and malware submission indicating "SUP" for support files.

Example: Support documents for the submission of malware for incident FB-10-0233 would have a zip file named "FB-10-0233 SUP.zip" (no password).

Below are instructions for creating a password protected compressed (zipped) folder in Windows XP using WinZip.

a. Without opening the file, save or copy it to your local desktop.

b. Right click on the file you intend to submit.

c. Go down to WinZip and choose “Add to Zip file…”

d. In the “Add to archive” text box, rename the file according to the procedures outlined above.

e. Select the box next to “Encrypt added files”. Click “Add”.

f. A WinZip caution window will pop-up, Click OK.

g. Enter the password “infected” (without quotes)

h. Reenter and confirm the password again.

i. Confirm encryption method 256-Bit AES encryption is selected and click OK.

Below are instructions for creating a password protected compressed (zipped) folder in Windows XP if you do not have WinZip.

a. Without opening the file, save or copy it to your local desktop then select the file.

b. Right click on the selected files and choose, Send to → Compressed (zipped) folder. Rename the compressed folder (.zip) per step “d” above.

c. Right-click the new compressed folder and select Explore.

d. From the File menu, select add a password.

e. Enter the password “infected” and click OK.

Tips for Identifying Spam

- Sending spam is a violation of the CAN-SPAM Act, *Title 18, U.S. Code, Section 1037*
- Information about cyber crime or filing a complaint may be found at: www.ic3.gov
- A list of common Internet fraud schemes is to be found here: http://www.ic3.gov/crimeschemes.aspx

- Common Internet fraud schemes include:
  Auction Fraud
  Credit Card Fraud
  Parcel Courier Email Scheme
  Employment/Business Opportunities
  Identity Theft
  Investment Fraud
  Nigerian Letter or "419"
  Phishing/Spoofing
  Reshipping

- Spams/scams are always evolving, and you may not readily recognize them
  - Some tips to determine if something is spam:
    - Check to see if they are asking for anything specific from your firm
    - If there is no indication of that, do a quick internet search
      - Check the sender's name, e-mail address, other information – they may come up as a known spammer

- Other tools:
  - FBI's website: www.fbi.gov/scams-safety/fraud/internet_fraud
  - IC3's website: www.ic3.gov/media/default.aspx
  - Be aware of some common tactics, such as creating a sense of urgency
    - Spammers use to trigger words to create that urgency
    - Urgent terms such as "notification" and "alert" are included in about 10 percent of attacks.

IC3 is a great resource for learning more about cyber crime. The IC3 was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate.

According to IC3, spam, or unsolicited bulk email, is now a widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others. It is usually considered unsolicited because the recipients have not opted to receive the email. Generally, this bulk email refers to multiple identical messages sent simultaneously. Those sending this spam are violating the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, *Title 18, U.S. Code, Section 1037*.

Spam can also act as the vehicle for accessing computers and servers without authorization and transmitting viruses and botnets. The subjects masterminding this Spam often provide hosting services and sell open proxy information, credit card information, and email lists illegally.

If you believe you may have fallen victim to this type of scam and wish to report it, you may file a complaint with IC3.

There are a number of common Internet fraud schemes, including credit card fraud, auction fraud, and investment fraud, and you may familiarize yourself with these schemes at IC3's site.

Spammers or scammers may trick you into clicking on a link or pop-up message in a spam email, or by getting you to visit a fake website set up solely to infect people's computers. Phishing scams are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality genuine organizations like a bank or a government authority will never expect you to send your personal information by an email or online. Scammers can easily copy the logo or even the entire website of a genuine organization. So don't just assume an email you receive is legitimate. If the email is asking you to visit a website to "update", "validate" or "confirm" your account information, be skeptical. Delete phishing emails. They can carry viruses that can infect your computer. Do not open any attachments or follow any links in phishing emails.

- Look for greetings that are generic. If it says something along the lines of "Dear Valued Customer" or "Dear [company name] Member," it is usually spam.
- Look for an email asking for personal information. Banks, eBay, Paypal and other online services make it very clear that they will NEVER ask you for your personal information, especially over email.
- The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. So, any e-mail you see from the IRS is almost certainly spam. The same is true for e-mails that say they are from the FBI.
- Remember, if you can identify an e-mail as spam, or a scam, it does not need to be reported to DSS
- But, if you can’t determine with ease that an e-mail is spam, err on the side of caution and report it via the SCR process to DSS