

VIRUS IDENTIFICATION SHEET

A computer virus is a program that downloads onto your computer without your consent or knowledge and spreads on its own. Viruses can cause you to lose cherished photos, videos, favorite music, and other important files you may have stored on your computer, and can sometimes be difficult to remove and cost you money.

Most viruses are the result of opening an infected email. In addition to keeping the information to the right in mind, follow these steps to help protect your computer from a virus:

1. Turn on your email's automatic HTML blocker, if it has one.
2. If available, set your email program to not automatically load images or remote content.
3. Do not blindly open emails or attachments.
4. Get an antivirus program, update it regularly, and replace every 2 years.
5. Think before you click!

SIGNS YOU MAY ALREADY HAVE A VIRUS

1. Your computer's operations are slow (please note that it's important to distinguish between the computer's operations and your internet connection.)
2. You are seeing many pop up ads.
3. Some files have mysteriously vanished.
4. Graphics and text are distorted.
5. Your computer randomly restarts.
6. Your friends and family receive emails from your email account that you did not send, containing suspicious web links and subjects.



Knowing when emails may have a virus:

1. You don't recognize the sender or the sender's email address.
2. The email is from a friend, family or vendor, but is unusual, unexpected, or out of character.
3. The sender's email address is a suspicious domain or the email contains a suspicious web link that is misspelled (like www.bankofarnerica.com. At first glance, it looks correct, but instead of an "m" in "America", they used an "r n". Or microsoftt-supportt.com, for another example).

4. Does the sender act as a representative of a bank, financial institution, the IRS, etc. and demand immediate payment?
(note: ALWAYS double check the validity of a claim from someone representing themselves as a banker, IRS agent, financial institution, etc! If in doubt, contact the institution directly.)



5. Is the subject line relevant to the content of the email?
6. Is the email message meant to look like a reply to something you never actually sent or requested?
7. Is the subject claiming you've won a prize or a "friend" is unexpectedly requesting money to help with transportation back into the country/hospital bills/etc.?
8. Is the list of people the email was sent to unfamiliar? Does the list follow a pattern such as all the last names are "Smith", or everyone's email address begins with a "C"?
9. Was the email sent at an unusual time, like 3 a.m.?
10. Does the sender threaten blackmail with a compromising or embarrassing photo that is attached?
11. Does the email have poor grammar and many spelling errors?
12. **Do you have a gut feeling that something is wrong?**