

Use Care When Reading Email with Attachments

You probably receive lots of mail each day, much of it unsolicited and containing unfamiliar but plausible return addresses.

Some of this mail uses *social engineering*¹ to tell you of a contest that you may have won or the details of a product that you might like. The senders are trying to encourage you to open the letter, read its contents, and interact with them in some way that is financially beneficial – to them. Even today, many of us open letters to learn what we’ve won or what fantastic deal awaits us. Since there are few consequences, there’s no harm in opening them.

Email-borne viruses and worms operate much the same way, except there are consequences, sometimes significant ones. Malicious email often contains a return address of someone we know and often has a provocative Subject line. This is social engineering at its finest – something we want to read from someone we know.

Email viruses and worms are common. If you’ve not received one, chances are you will. Here are steps you can use to help you decide what to do with every email message with an attachment that you receive. You should only read a message that passes all of these tests.

1. The **Know** test: Is the email from someone that you know?
2. The **Received** test: Have you received email from this sender before?
3. The **Expect** test: Were you expecting email with an attachment from this sender?
4. The **Sense** test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender – let’s say your Mother – to send you an email message with the Subject line “Here you have, ;o)” that contains a message with attachment – let’s say *AnnaKournikova.jpg.vbs*? A message like that probably doesn’t make sense. In fact, it happens to be an instance of the **Anna Kournikova worm**, and reading it can damage your system.
5. The **Virus** test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program. That task is described in Task 1 – Install and Use Anti-Virus Programs (<http://www.cert.org/homeusers/HomeComputerSecurity/#1>).

¹Social engineering is the art and science of getting people to comply to your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behavior and it is far from foolproof. (From <http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html>)

You should apply these five tests – **KRESV** – to every piece of email with an attachment that you receive. If any test fails, toss that email. If they all pass, then you still need to exercise care and watch for unexpected results as you read it.

Now, given the **KRESV** tests, imagine that you want to send email with an attachment to someone with whom you've never corresponded – what should you do? Here's a set of steps to follow to begin an email dialogue with someone.

1. Since the recipient doesn't already **Know** you, you need to send them an introductory email. It must not contain an attachment. Basically, you're introducing yourself and asking their permission to send email with an attachment that they may otherwise be suspicious of. Tell them who you are, what you'd like to do, and ask for permission to continue.
2. This introductory email qualifies as the mail **Received** from you.
3. Hopefully, they'll respond; and if they do, honor their wishes. If they choose not to receive email with an attachment from you, don't send one. If you never hear from them, try your introductory email one more time.
4. If they accept your offer to receive email with an attachment, send it off. They will **Know** you and will have **Received** email from you before. They will also **Expect** this email with an attachment, so you've satisfied the first three requirements of the **KRESV** tests.
5. Whatever you send should make **Sense** to them. Don't use a provocative Subject line or any other social engineering practice to encourage them to read your email.
6. Check the attachments for **Viruses**. This is again based on having virus-checking programs, and we'll discuss that later.

The KRESV tests help you focus on the most important issues when sending and receiving email with attachments. Use it every time you send email, but be aware that there is no foolproof scheme for working with email, or security in general. You still need to exercise care. While an anti-virus program alerts you to many viruses that may find their way to your home computer, there will always be a lag between when a



virus is discovered and when anti-virus program vendors provide the new virus signature. This means that you shouldn't rely entirely on your anti-virus programs. You must continue to exercise care when reading email.

Use the checklist from

<http://www.cert.org/homeusers/HomeComputerSecurity/checklists/checklist3.pdf>

to help you make decisions about opening email attachments.

This article is adapted from task 3 in "Home Computer Security," which can be found at

<http://www.fedcirc.gov/library/documents/homeusers/index.html>

and at

<http://www.cert.org/homeusers/HomeComputerSecurity/>.

This work was funded by the General Services Agency of the U.S. Government.

Copyright 2003 Carnegie Mellon University

CERT is registered in the U.S. Patent and Trademark Office.