Chain Letters and Hoax Sites

Let's talk about chain letters.

We've all received them as they circulate in cyber-space making unbelievable claims of get rich quick schemes, amazing cures for diseases and heartbreaking stories of sick and missing children.

Internet hoaxes and chain letters are e-mail messages written with one purpose: to be emailed to everyone in your address book.

They often contain bogus warnings usually intent only on frightening or misleading readers.

Chain letters and hoax messages all have a similar pattern.

From the older printed letters to the newer electronic kind, they all have three recognizable parts: a hook, a threat and a request.

The Hook

First, there is a hook to catch your interest and get you to read the rest of the letter.

Some examples of Hooks are: "Make Money Fast" or "This Message Could Save Your Life."

The Threat

When you are hooked, you read on to the threat.

Most threats warn you about the terrible things that will happen if you do not maintain the chain.

The threat often contains official or technical sounding language to deceive you into believing it is real.

The Request

Last is the request.

Some older chain letters ask you to mail a dollar to the top ten names on the letter and then pass it on.

Electronic versions direct you to "Distribute this letter to as many people as possible."

We have to wonder, "Why do people send chain letters and hoax messages"?

Only the original writer knows the real reason, but some possibilities are:

- ➢ To see how far the letter will go
- ➢ To harass another person
- ➢ To trick money out of people using a pyramid scheme
- ➢ To kill some other chain letters
- ➢ To damage a person or organization's reputation
- ➢ And most likely the real reason: to expose email addresses to spammers, scammers and predators

Asking for money or product is illegal in a chain letter.

Legitimate warnings about crime trends, health concerns, missing persons, computer viruses and network problems are often sent out

in chain letters in a misleading and frightening manner.

Typically, police, health officials and computer companies will issue warnings and notifications in a more timely and effective manner, and they will often validate their warning message on their company website.

Kids are especially at risk of believing chain letters because they often offer them good luck or devastating consequences to their family if they do not forward the message or comply.

Websites such as Snopes or Hoaxbusters specialize in uncovering urban legends.

It is often surprising to read stories on these sites that we have received in an email and originally believed them to be true.

Spammers, scammers and predators are always searching for email addresses on the Internet for which to prey on.

Before forwarding emails, get in the habit of deleting past recipients, then post your address book into the BCC mode (Blind Carbon Copy) or into a folder of undisclosed recipients prior to forwarding emails onward.

Monitor your children's kids email addresses and make sure their address is age and gender neutral and ensure if you are inserting a signature in an email message it does not disclose personal information like a home phone number or address.

The best course of action is to delete chain messages and help keep cyberspace free of misleading and potentially harmful information.

Even though these messages seem innocent, there is already too much junk mail, SPAM and political incorrectness on the Internet which harms us all.