

SCAM ALERT #8

Phishers reeling in unknowing IMers

Next time you see your son or daughter sending an instant message (IM) to a friend, consider this: **reports indicate that phishers have discovered the instant messaging waters, and your child could be the next victim.**

Pulling them in

The same way you might be tempted to click on a pop-up ad, your teen might think it's safe to accept an IM from a stranger, and then click on a link to what looks like a site they are familiar with. The danger lies in the fact that these "fake" sites look like the original site being copied, and phishers are enticing your child to provide personal information about themselves, or even your entire family.

Don't take the worm

While instant messaging can be an efficient, cost-effective way for your teens to chat, it can also be dangerous if they aren't careful. Share these helpful tips with your teen to keep them – and your family – safe.

Please consider the following tips and share them with anyone in your household who uses IM.

NEVER!

- accept messages from screen names you don't recognize.
- agree to meet a stranger in person that you met on IM.
- accept files or downloads from people you don't know.
- post your screen name on line.
- provide personal or private information, like your Social Security Number, account numbers or passwords, or even just your address via IM.

SEFCU is committed to helping members protect themselves against fraud. This is the eighth in a series of SCAM ALERTS to educate members about deceptive activities that could harm members' financial security. While we cannot advise members of every scam, we hope the series will advance awareness of privacy and security issues.

©SEFCU, April 2005