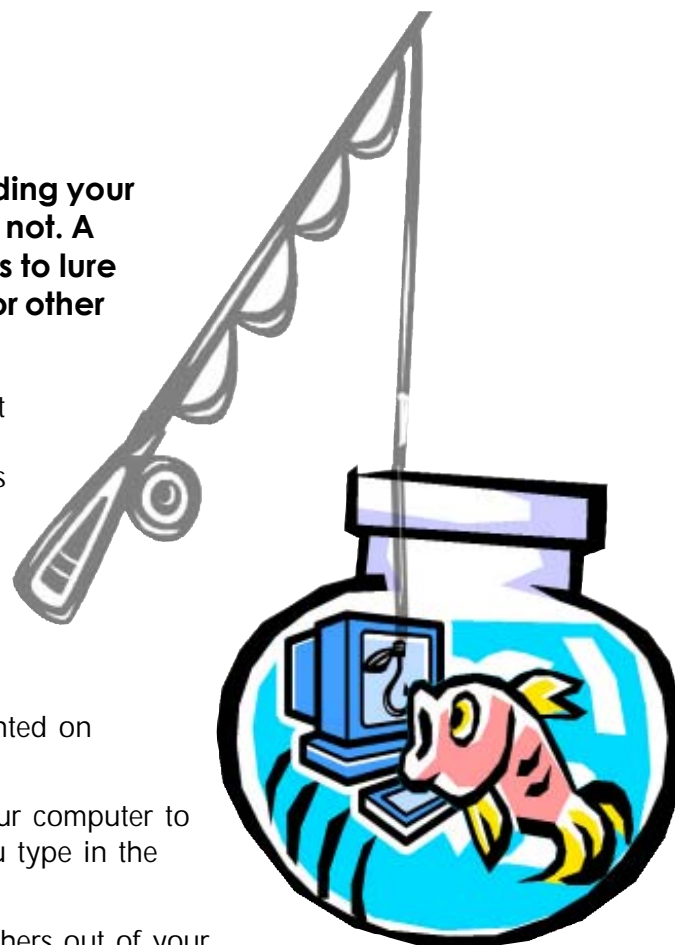


phishing

“Phishing” is when identity thieves try to trick you into providing your personal information by pretending to be someone they’re not. A phishing scam involves sending spam or pop-up messages to lure credit card numbers, Social Security numbers, passwords, or other sensitive information from Internet users.

- Legitimate companies, organizations, or government agencies won’t contact you unexpectedly asking for your personal information. If you get a call or email like that, contact whoever the person claims to represent directly by phone or email to verify the request.
- Don’t click on links in emails asking for your personal information. They may lead you to fake versions of legitimate Web sites, where criminals hope you’ll hand over your personal information.
- Never enter your information in pop-up screens. They may be planted on legitimate Web sites by identity thieves.
- Beware of “pharming,” con artists secretly planting programs in your computer to hijack your browser and take you to phishing sites, even when you type in the Web address yourself!
- Keep malicious messages and programs that could be used by phishers out of your computer with a spam filter, up-to-date anti-virus and anti-spyware software, and a strong firewall.
- For more tips about phishing, go to www.phishinginfo.org and www.onguardonline.gov.





These tips about phishing are brought to you by Verizon (<http://netservices.verizon.net>).

october07

sunday	monday	tuesday	wednesday	thursday	friday	saturday
	1	2	3	4	5	6
7	8 Columbus Day	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28 Daylight savings time ends	29	30	31	NCL 100+ YEARS CONSUMER EDUCACY National Consumers LEAGUE		