Social Networking the Safe Way

Many of us at iolo use online social and professional networks, and these sites continue to grow in popularity worldwide. According to The Nielsen Company, the amount of time people spend on blogging and social networks increased 210% over the past year, with the leading sites boasting hundreds of millions of users.

These virtual communities are a great way to stay connected with friends and family, but unfortunately they also can connect us to scam artists.

Thieves are devising increasingly clever ways to use these sites to run cons. They'll hack into an account, pass themselves off as your friend, and then trick you into downloading malicious software.... or they'll make a desperate, emergency plea for you to send them cash to a mail box... or they'll run a phishing scam that leads you to a fake web site that asks for private banking information.

Another ploy are the quizzes and games that ask for your cell phone number so that the results can be sent to you—and you don't know you've been conned until you see mysterious charges on your next phone bill.

If you're a victim of fraud or identity theft...

- **Immediately close all of your credit card and bank accounts.**
- **Change all of your passwords and PINs.**
- **Contact one of the consumer credit reporting companies and place a fraud alert on your credit report: Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289.**
- **Get a replacement driver's license.**
- **Report any crimes to the police and keep a copy of the report to give to creditors.**

- From USAA Financial Services

Protect yourself

- Avoid being "click happy": if something you get from a friend looks strange—an odd-looking web address or wording that doesn't sound like something they'd write—double-check with them, in-person or over the phone, and ask if they sent you the message.
- Limit what you share on your profile page or as part of online games. Revealing information like birth dates, cell phone numbers, and travel plans can expose you to all kinds of criminal activity, including identity theft, stalking, and home robbery.
- Be selective about who you accept as a friend on social sites. Identity thieves often create phony profiles with the sole intent of capturing people's private information.
- To avoid your own account being hacked into, protect your login information and use strong passwords that you change frequently.
- Don't use the same password for these sites that you use for your bank accounts or work login: if someone figures out your password for the social site, that person now has access to everything else.
- Install and run anti-malware software and enable the real-time feature to automatically block any malicious files.