



Social Media Scams

From the Office of Minnesota Attorney General Lori Swanson

Social media has become an important part of many of peoples' lives. In an instant, it lets people share photos with family members, catch up with old friends, and get the daily news. Despite its positive aspects, social media has also become a tool used by scam artists to take advantage of people. As the prevalence of social media scams increases, you should know what to look for. Here are a few examples of common social media scams:

“Click Bait” Scams.

“Zach” checked his social media feed and saw a post titled, “See backstage photos from last night’s concert!!” He “clicked” on the post and a pop up browser opened that instructed him to “click” a link to update his photo viewer. After Zach “clicked” the link, his antivirus software informed him that it had blocked an attempt to install malware on his computer. He immediately logged out of his account, closed his browser, and ran a full scan of his computer using his antivirus software. The scan found no threats, so Zach logged back into his social media account and changed his password and security questions.

Impersonation Scams.

After logging into her account, “Nora” received a private message from her best friend “Margie” that said she had lost her purse while on vacation in another country and asked her to send a \$600 wire transfer to help pay for her hotel room. Nora was supposed to have dinner with Margie that night, so she knew the story could not be true. When she called the real Margie, Nora learned that a scam artist had hacked Margie’s account and used it to send the messages.

Online Dating and Romance Scams.

“Jason” received a friend request from a stranger named “Emily.” After Jason accepted the request, Emily claimed to be an American on business in Germany. They seemed to hit it off and began to plan a road trip for that summer when Emily would come back to the U.S. Emily sent Jason a \$5,000 check to cover the cost

of the trip, but then suddenly asked him to send \$4,500 back to her because she had been laid off from her job and needed the money for rent. Jason deposited the check and wired the money, but was soon contacted by his bank, which told him the check was fraudulent and he had to repay the \$4,500. On top of losing the money, the fake “Emily” disappeared and Jason never heard from her again.

Quizzes and Polls.

“Laura” saw a post on her social media feed post titled, “Win a free TV.” She “clicked” on the link in the post and was forwarded to a website that instructed her to answer three questions and enter her name, telephone number, address, bank account number and Social Security number to be entered to win the free TV. Laura realized that this information could be used to commit the crimes of theft and identity theft, so she closed the browser and logged out of her account.

Phishing Scams.

“Tim” received an email that purported to be from his favorite social media website. The email said that his account had been locked and asked him to “verify” his account by “clicking” a link. After he “clicked” on the link, Tim was forwarded to a webpage that had the same graphics and color scheme as the social media website. The webpage directed Tim to enter his username and password to verify and unlock his account. He entered this information before realizing he was on the wrong website. Tim then contacted the social media website at the email address listed on its real webpage and it helped him recover his account.

Sweepstakes and Lottery Scams.

“Anna” received a chat message while on her social media account from an individual who claimed that she won \$100,000 in a lottery sponsored by the social media website. The individual told Anna that she needs to send \$750 via a reloadable card to pay the taxes and fees on her winnings. Because she had not entered any lotteries,

Anna knew that she could not be a winner. She closed the chat session and reported the individual to the social media website.

Work at Home and Other Money-Making Schemes.

“Heather” received a post from an individual who claimed his company could help her make thousands of dollars from home every week if she invested a “small” amount of money. After she expressed interest in the program, the individual asked for Heather’s credit card number to pay \$19.99 for a startup kit. Heather provided the information, but never received the promised materials. When she checked her credit card account statement several months later, she discovered that, in addition to the \$19.99 fee, the company had also charged her a \$99.99 membership fee every month. Heather disputed the charges with her credit card company, which reversed the charges and changed her account number.

How to Avoid Social Media Scams

1. Don’t take the “bait.” Never “click” on pop-up messages, posts that contain content that seems shocking, scandalous, or too good to be true, or links or attachments in unsolicited emails and text messages.
2. Create a strong password. This means that it is a minimum of seven characters in length and contains a mixture of upper and lower case letters, symbols, and numbers. You should never provide your password to someone you do not know.
3. Don’t provide your information (personal or financial) online unless you know the website you are using legitimate, secure, and encrypted. It is also important to make sure that you are dealing with the right entity, and using its real website and not a look-a-like site created by a scam artist. Also, look for “https://” (the “s” is for secure) before a web address.
4. Disregard unsolicited emails and text messages that request personal or account information. Companies you do business with already have this information and do not need to verify or confirm it. In the event

of a security breach, most companies contact their customers in writing to alert them to the matter.

5. Contact companies through trusted channels. If you are concerned about an email or other message you received, call the company immediately at its publically-listed phone number. Never trust the phone number or email address in the message.
6. Verify the person you are dealing with is who they claim to be, and not an imposter. Contact a friend or family member who could confirm the person’s story, or try contacting the real person at a phone number you know is accurate.
7. Don’t be rushed into sending money immediately or secretly. Refuse to send money through wire transfer, overnight delivery, or reloadable cards unless you are absolutely certain that you are sending money to a real friend or family member.

Taking Action

If you are a victim of a social media scam, take the following steps:

- ✓ Cease all contact with the scam artist and block his or her phone numbers, instant messages, and email addresses.
- ✓ Keep copies of all communications.
- ✓ Report the matter to the social media website.
- ✓ Report the matter to your local police department.
- ✓ Report the matter to the Federal Bureau of Investigation’s Internet Crime Complaint Center online at www.ic3.gov.
- ✓ Report the matter to the Federal Trade Commission as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
Toll free helpline: 1-877-382-4357
Website: www.consumer.ftc.gov

For additional information, contact the Office of Minnesota Attorney General Lori Swanson.