OUCH! April 2025

Account Takeovers: Emotional Predators

Caught off Guard: Emma's Story

Emma was scrolling through Facebook when she saw a heartfelt post from her cousin, Sarah. The post shared devastating news: Sarah's elderly father had moved into a retirement care facility and was selling his belongings to help cover medical expenses. Included were pictures of items like his car, jewelry, and vintage furniture at unbelievably low prices.

Wanting to help and score a great deal, Emma quickly contacted Sarah through Facebook Messenger for the first time in years. Sarah was glad to hear from her cousin and updated Emma on her father's condition. Sarah quickly moved on to payment details, urging Emma to act fast since many items were already spoken for. Emma quickly sent the money, only to discover later that the entire post was a scam.

Emma had never actually been talking to her cousin. Sarah's Facebook account had been hacked and taken over by a scammer. After gaining full access, the scammer posted fake news about Sarah's father and then exploited Sarah's trusted network of friends and family by pretending to sell his items. When people thought they were buying items from Sarah (and supporting her father), they were really paying a scammer who simply walked away with their money.

What's Happening?

Scammers are hijacking social media accounts on platforms like Facebook or Instagram, often by figuring out username and passwords. Once inside, they pose as the account owner to share fake posts that often include emotional details to create a sense of urgency and drive people into action. These scams often include stories like being mugged in a city and needing help, or being in a car accident and needing money, or that a loved one passed away and their belongings are being sold.

Victims are drawn in, believing the post is from someone they know and trust. They send money, often via untraceable payment methods like peer-to-peer apps or wire transfers, only to later find out they were not really dealing with their family or friends, and their money is gone.

What Makes Scams Like These So Dangerous?

- **Hijacked Trust**: Scammers leverage the trusted network of the social media accounts they take over. Posts appear to come from a trusted friend or family member, making them more believable.
- **Emotional Manipulation**: Scammers use personal and emotional topics that often create a strong sense of urgency or opportunity, pressuring people into ultimately making a mistake.

- **Rapid Spread**: Once a victim's account is compromised, the scammer can quickly reach hundreds if not thousands of people. In addition, many people use the same password for multiple social media accounts, so once one account is taken over, that same password can be used to take over the victim's other social media accounts.

How to Protect Yourself and Others

- **Be Skeptical of Emotional Posts Involving Money**: If a post seems unusually emotional or urgent and involves sending someone money, pause and verify, it could be a scam.

- **Verify with the Person Directly**: Contact the person through a separate channel to confirm the story. For example, call them on the phone or speak with them in-person. Quite often, the victim does not even know their account has been taken over or about the scammer's posts on their account.

- **Check for Red Flags**: Scammers often ask for payment through untraceable methods such as gift cards or Bitcoin. Another red flag is if they ask you to use a different platform to continue communications (such as moving from Facebook Messenger to WhatsApp).

- **Protecting Your Account:** If your account is hacked and taken over, the first thing cyber criminals often do is change your password, locking you out. Once that happens it is very difficult to recover your account. Start by protecting each of your accounts with a long and unique password. Then enable multi-factor authentication for each account. These two simple steps make your accounts far more secure, and scammers will hate you for it!

Stay One Step Ahead

When it comes to account takeover scams, you are your own best defense. If you suspect you've encountered this scam, report the account and notify your social media platform immediately.

Guest Editor

Amie Dsouza is a cybersecurity professional working with a major US Airline. She has worked in six countries and serves as a board member for Women in Cybersecurity (WiCys). Amie actively advocates for educating everyone on keeping personal data safe online.

Resources

Emotional Triggers: How Scammers Trick You: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
How Cyber Criminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords
The Power of the Passphrase: https://www.sans.org/newsletters/ouch/power-passphrase/
I'm Hacked, Now What?: https://www.sans.org/newsletters/ouch/im-hacked-now-what/