OUCH! December 2024

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Unveiling the Shadows: How Cyber Criminals Steal Your Passwords

A Digital Nightmare: Lisa's Unwanted Exposure

Lisa, a graphic designer with a knack for creativity, lived much of her life online. She managed her banking, shopping, and social interactions through various apps and websites. One day, she noticed some strange withdrawals from her bank account — items she'd never bought from stores she'd never visited. Her social media accounts then began posting spam messages promoting odd products and services, and friends reported receiving unusual emails from her.

Panic set in as Lisa realized she had lost control over her digital identity. Her personal photos were leaked, and private conversations were exposed. Clients began to question her reliability, and her reputation took a hit. After consulting with cybersecurity experts, Lisa discovered that her passwords had been compromised. Cybercriminals had gained access to her most sensitive accounts, unraveling her digital world piece by piece. The question lingered: How did this happen?

The Underhanded Tactics of Cybercriminals: Five Common Methods

Cyber threat actors employ a variety of techniques to harvest passwords. Here are five common ways they could obtain yours like they did Lisa's:

1. **Social Engineering Attacks**

   Social Engineering is where attackers masquerade as someone or something you know or trust, and they trick you into doing something you should not do. They send emails or messages that appear legitimate, often creating a strong sense of urgency, fear, or curiosity.

   How It Happened: Lisa received an email that looked like it was from her bank, complete with official logos and branding. The email claimed there was suspicious activity on her account and urged her to click a link to verify her identity. The link led to a fake website that captured her login credentials when she entered them.

2. **Malware**

   Malware is malicious software designed to infect computers. Once infected, cyber criminals can do whatever they want. Keyloggers (sometimes called *information stealers*) are a type of malware that record every keystroke made on a device, including your login, passwords, and other sensitive data.

   How It Happened: Lisa downloaded what she thought was a legitimate font package for her design work. Hidden within was a keylogger that installed itself on her computer. Over time, it recorded her login details for various accounts and sent them back to the attacker.

3. **Brute Force Attacks**

   In brute force attacks, cybercriminals use automated tools to try numerous password combinations until they guess the correct one. Weak passwords are especially vulnerable to this method.

   How It Happened: Lisa used simple passwords like "lisa2020" for many of her accounts. Attackers used software that systematically tried common passwords and easily cracked her accounts.

4. **Data Breaches**

   When a website or service gets hacked, it can affect everyone's accounts that may be stored on the server. If someone uses the same password for multiple accounts, when that password is compromised for one account, then that password can be used to access the victim's other accounts as well.

   How It Happened: A popular social media platform Lisa used experienced a data breach. Since she used the same password elsewhere, attackers accessed her other accounts using the leaked credentials.

5. **Purchased Credentials**

   Cyber criminals can simply buy your passwords on the internet, often on the Dark Web. Certain cyber criminals specialize in stealing victims' passwords, using any of the methods we discussed so far. They then store and sell the stolen passwords to other cyber criminals.

   How It Happened: A cybercriminal decided they wanted to make as much money as possible over the weekend, so they went to the Dark Web and purchased over 100,000 compromised accounts with their full passwords. One of Lisa's accounts was on that list.

Three Key Steps You Can Take

Fortunately, by taking three simple steps, you can go a long way to protecting your accounts and online, digital life.

1. Use a long, unique password for each of your accounts. We recommend passphrases, which are long passwords made up of multiple words.
2. Use a password manager to securely store and manage all those passwords for you.
3. Enable Multi-Factor Authentication (MFA) whenever possible for your most important online accounts.

Guest Editor

Lekshmi Nair is a senior Cybersecurity leader with 22 years of rich experience in Information Security Consulting and Cybersecurity Strategy. She is currently a Sr. Director of Application Security Consulting with BlackDuck Software. She is the founder and President of WiCyS India.

Resources

Phantom Voices: Defend Against Voice Cloning Attacks: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Text Messaging Attacks: A Smishing Saga: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
Top Three Ways Cyber Attackers Target You: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
The Power of Passphrases: https://www.sans.org/newsletters/ouch/power-passphrase/
The Power of Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/