How to Handle Online Scams and Hacks: A Guide to Protecting Yourself and Involving Law Enforcement

Please email Wyoming SBDC Cybersecurity Program Manager Paul Johnson or call 307-314-5208 for further assistance for protecting yourself against and handling online scams or contact your SBDC Advisor for assistance. Visit the Wyoming SBDC Network website for comprehensive small business assistance.

Introduction:

In today's digital world, scams and hacking attempts are unfortunately common. Whether it's a phone call claiming to be from your bank, an email promising a prize, or someone stealing your personal information, becoming a victim can be overwhelming and frustrating. However, knowing how to respond quickly and effectively can make all the difference in stopping the scammer and protecting yourself from further harm.

This guide will walk you through the steps of what to do if you've been scammed or hacked, how to know when to involve law enforcement, and what information you will need to supply law enforcement. We'll also cover practical tips for avoiding scams in the future so you can stay one step ahead of online threats. Whether you've lost money or just want to make sure your data stays secure, this guide will help you navigate the process with confidence and ease.

When to Contact Law Enforcement

You should consider involving law enforcement if you experience any of the following*:

- **Significant financial loss —** You've lost a large amount of money (especially if it's over $1,000).
- **Identity theft —** Someone is using your personal information, such as Social Security numbers, bank account details, or credit card info, without your permission.
- **Harassment or threats —** If the scam or hacker is threatening you or stalking you, whether online or by phone.
- **Criminal activity —** If you think a crime, such as fraud or wire transfer fraud, has taken place.
- **Scammer known location —** If you have enough information to know where the scammer is located (even if they're out of the country), law enforcement can help track them.

* The SBDC's staff cybersecurity expert and Certified Ethical Hacker recommends that you contact your attorney before involving law enforcement. Your attorney is probably the best person to advise what exact steps to take when and if you involve law enforcement officials.

When Not to Involve Law Enforcement

Involving law enforcement may not be necessary in the following cases:

- **Minor financial loss —** If the scam or hack resulted in a very small loss (usually under $1,000), you might be better to handle the situation through your bank or service provider.
- **Limited personal info exposed —** If you don't believe your personal info was stolen or misused, don't involve law enforcement.
- **Already reported —** If you've already reported the theft or attack to your bank, credit card company, or the service provider who can take action (e.g., freezing accounts or credit monitoring).

What Information to Provide to Law Enforcement

Be prepared to give the following details:

- **Personal information —** Name, contact details, and if relevant, any documentation showing identity theft (such as changes to accounts, unauthorized transactions, etc.).
- **Details of the scam or hack —**
  - How and when it happened.
  - What you were told by the scammer (e.g., emails, phone calls, etc.).
  - The method of contact (phone, email, text, website, etc.).
- **Financial details —** If money was involved, provide any receipts, account transactions, or statements showing the transfer.
- **Suspect info —** If you have any details about the scammer's location, name, or even their contact info.
- **Evidence —** Keep a record of everything related to the scam or hack (screenshots of emails, texts, photos, or links).

What Questions Law Enforcement May Ask

Expect questions like these:

- When did you first notice the scam or hack?
- What happened during the incident? Can you describe what the scammer said or did?
- Were you asked for money, passwords, or other sensitive info?
- Have you reported the incident to your bank, credit card company, or another service provider?
- Do you have any tangible evidence (emails, texts, transaction records, screen shots) to prove a crime was committed?
- Was there any unusual activity on your accounts or devices prior to noticing evidence of the incident?

Practical Tips for Dealing with Scammers and Hackers

- **Don't respond to unsolicited calls or messages —** If someone contacts you unexpectedly, especially asking for personal information, don't engage. Hang up or delete the message.
- **Verify before you act —** If you get an email or phone call from a "company" asking for sensitive details, verify the contact by calling them directly through official numbers from their website.
- **Use strong passwords and change them regularly —** Make sure your passwords are long, complex, and unique for each account. Consider using a password manager. Do not use a web browser to manage passwords. A dedicated password manager is likely more secure and employs encryption techniques a web browser does not.
- **Enable multi-factor authentication (MFA) —** For added security, use MFA wherever possible to add an extra layer of protection to your accounts.
- **Monitor accounts and credit reports —** Regularly check your bank accounts, credit card statements, and credit reports for any unauthorized activity. Many services allow you to sign up for alerts on new activity.

How to Prevent Future Scams and Hacks

- **Educate yourself about common scams —** Familiarize yourself with the latest scams and methods hackers use (e.g., phishing emails, fake tech support calls).
- **Install antivirus and anti-malware software —** Ensure your computer and devices have protection against viruses and malware.
- **Use a secure Wi-Fi connection —** Avoid using public Wi-Fi for sensitive activities like online banking. Consider using a VPN when using public Wi-Fi.
- **Back up your data —** Regularly back up important files to prevent losing them in case of a cyberattack. Ideally, use cloud backups with multiple redundancies and automatic backup capabilities.

Conclusion:

Dealing with online scams or hacks can be stressful, but with the right knowledge and tools, you can take steps to secure your accounts, knowing how to act quickly and responsibly is crucial. By staying informed about common threats and following the preventive tips outlined in this guide, you can strengthen your defenses and reduce your chances of becoming a victim again.

Remember, the key to staying safe is vigilance; never hesitate to report suspicious activity and always verify information before acting. If you do fall victim to a scam or hack, take action right away, and don't hesitate to reach out to the proper authorities.

For more information on how to protect yourself from cyber threats, check out these resources:

- Federal Trade Commission - Consumer Advice on Scams

- Cybersecurity & Infrastructure Security Agency (CISA)
- Identity Theft Resource Center
- Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center (IC3)
- Better Business Bureau - Scam Tracker

Stay safe, stay informed, and take action when needed! And contact your Wyoming SBDC advisor for personal, no-cost advising on any cybersecurity matter.