I've been hacked! Who do I call?

Cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. According to the 2015 Verizon Data Breach Report, intrusions go undetected more than 200 days from the actual event. Some criminals disband one criminal operation—only to start up a new activity with a new tactic —before an incident even comes to the attention of the authorities. Once you believe you have been the victim of a cybercrime, it's important to report it and to protect the evidence.

Who to contact:

Local law enforcement. Even if you have been the target of a multi-jurisdictional cybercrime, call your local law enforcement agency (either police department or sheriff's office). They have an obligation to help you, take a formal report, and make referrals to other agencies. Report your situation as soon as you find out about it. Some local agencies have detectives or departments that focus specifically on cybercrime.

Seek Legal Advice. If you are a business owner, seek legal advice to guide you in addressing whatever liability and reporting requirements govern the breach. Protecting sensitive employee data, health data, or credit card data have various governing regulations and notification requirements.

IC3. The Internet Crime Complaint Center (IC3) will thoroughly review and evaluate your complaint and refer it to the appropriate federal, state, local, or international law enforcement or regulatory agency that has jurisdiction over the matter. IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance). Complaints may be filed online at http://www.ic3.gov/default.aspx.

What to collect:

Even though you may not be asked to provide evidence when you first report the cybercrime, it is very important to keep any evidence you may have related to your complaint. Keep items in a safe location in the event you are requested to provide them. Evidence may include:

- Canceled checks and copies of bank statements
- Certified or other mail receipts

- Credit card receipts
- Envelopes (if you received items via FedEx, UPS, or U.S. Mail)
- Faxes
- Log files, if available, with date, time and time zone
- Messages from Facebook, Linkedin, Twitter or other social networking sites
- Money order receipts
- Pamphlets or brochures
- Phone bills
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages (to prove web defacement)
- Wire receipts

And most importantly, don't shut down your computer or erase any files. Law enforcement and/or a computer forensic specialist will need the evidence stored on your hard drive and memory storage locations.

A Word about Malware:

Many cybercrimes start with malware—short for "malicious software." Malware includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent—you may have downloaded the malware without even realizing it! These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information and commit fraud. If you think your computer has malware, you can file a complaint with the Federal Trade Commission at www.ftc.gov/complaint. Often malware is embedded in links to emails or attachments. Don't open an attachment from someone you don't know!

Tips for a Small Business:

Small businesses are particularly vulnerable to a cyber attack because they typically have fewer financial and human resources than larger firms. While all businesses are subjected to some levels of risk, smaller firms are less resilient due to this lack of resources. This is why it is important to start now to protect yourself and your business from an event that may have disastrous consequences. Protecting your most critical assets before they are stolen; building a recovery plan; and learning how you and your employees can stay safe online are the first steps to preventing a cyber attack.