RIVERBANK
We Bring Banking to You!

# UNDERSTANDING CYBERCRIME

**What is cybercrime and how does it work?**
Cybercrime is a lucrative trade and it's growing. Criminals have identified where the money is and, as a result, cybercrime is quickly becoming a major threat. Millions of dollars are lost every year. Because these criminals continue to refine and fine-tune each element of the cybercrime supply chain, users must be educated and alert. The more we know about cybercrime, the better equipped we will be to defend against it; and the best way to do that is to understand who the typical perpetrators are, what motivates them and what methods they use to perpetrate their crimes.

**How can my information be compromised?**
The most common way to steal confidential information is by embedding spyware programs on computers. These programs log and track keystrokes and capture user names, passwords and PINs and send the information to hackers who sell it on the black market. But there are many other ways that information is compromised.

In short, the massive amount of personal information online, coupled with the lack of user knowledge of how to secure this data makes it easy for cybercriminals. They use a variety of technologies to obtain your information including password crackers, keyloggers, malware, and a variety of social engineering techniques.

**How can I protect myself?**
Follow these guidelines to help you ensure that your information remains safe.

1. **Keep your firewall turned on.** A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information.
2. **Install or update both anti-virus and anti-malware software.** You need both to prevent malicious software programs from embedding themselves on your computer. Set them to update automatically.
3. **Install or update your antispyware technology.** Some spyware collects information about you without your consent; others produce unwanted pop-up ads on your web browser.
4. **Keep your operating system up to date.** Updates are needed to fix security holes.

5. **Be careful what you download.** Careless downloading documents, images and apps can beat even the most vigilant anti-virus/ anti-malware software.
6. **Close your browser when you’re done working.** Delete the cache, history and passwords each time. Also, turn off your computer. Turning the computer off effectively severs an attacker's connection.
7. **Monitor your credit.** Since you can’t protect information that's in the hands of myriad of organizations, you need to monitor your credit reports. For even more protection, you might consider a credit monitoring service that will alert you when there’s an entry in your credit file.
8. **Ignore scareware.** Scareware pop-ups may look like actual warnings from your system, but they’re not. Made to appear authentic, they often deliver malicious payloads. Close them with the “X” button.
9. **Review your bank and credit card statements.** It’s one of the easiest ways to notice if something is wrong.
10. **Choose strong passwords.** And don’t use the password you use for online banking anywhere else. Change your most critical passwords every 90 days.

MySECURITY
Awareness.com