Fraud threatens not only companies and organizations, but also individual consumers as they go about their daily lives – both online and off.

1. If you get a voice mail from your credit card company asking you to call back, only call back using the number listed on the back of your card. Never respond directly to the contact number offered in the message.

2. Websites with questionable content will sometimes ask for a credit or debit card number "for identification purposes only". Don't get tricked into giving up this information. Unless you are actually making a purchase, there is no need to share your credit card information.

3. Don't be burned by a phish. Be suspicious of any emails from a bank or credit card company requesting your account information. Contact the company directly (and not through the unsolicited email) to confirm the request.

4. Perform periodic checks on your internet browser and social media sites to ensure your privacy settings still match your needs. After visiting secure websites, clear the cache of your browser so no one can view any sensitive information.

5. Do not click on 'unsubscribe' links in any unsolicited email, or reply with an unsubscribe message. Doing either will simply confirm to the spammer/scammer they are reaching a live email address and they will continue to keep you on their contact lists. Instead, simply delete the email or move it to "Junk".

6. There are two simple signs you're secure while shopping online. One is the "padlock" icon located at the top of your browser window, the other is "https" in the address bar. These confirm the page you are on is secure and your data will be encrypted.

7. Become a password power user. Avoid obvious passwords like birthdays, addresses or phone numbers – these aren't just easy to guess, they're easy to get with simple searches. Most sites recommend (or even require) a minimum of eight characters and a mix of numbers and letters.

8. Don't use repeat passwords for anything involving sensitive personal information. Fraudsters will run compromised email accounts against financial institutions in case there is a repeat which will grant them access.

9. Change your passwords frequently. Many sites require periodic password changes and don't permit password recycling. Just as you change your smoke alarm batteries every year, make it a habit to change your passwords every few months.