



## ONLINE SECURITY TIPS FOR CARDHOLDERS

Shopping online with Visa is a simple, convenient, and safe way to make purchases, 24 hours a day, seven days a week. Consider these basic steps to help you avoid risk and stay secure when you're online—whether you're using email or shopping at your favorite merchant.

- Protect your Visa card with Verified by Visa. Added password protection helps ensure that only you can use your Visa card online.
- Be discriminating when providing personal information online. Never give out your personal or account information to anyone you do not trust. And make sure to verify a business's legitimacy by visiting its web site, calling a phone number obtained from a trusted source, and/or checking with a reliable resource.
- Keep your passwords secret. Some online stores may require you to register with them via a user name and password before buying. Online passwords, including your Verified by Visa password, should be kept secret from outside parties the same way you protect your ATM PIN.
- Look for signs of security. Identify security clues such as a lock image at the bottom of your browser, or a URL that begins with https://. These signs indicate that only you and the merchant can view your payment information.
- Only give your card details when you initiate a purchase - do not provide them for any other reason.
- Never send payment information via email. Information that travels over the Internet (such as email) is not fully protected from being read by outside parties. Most reputable merchant sites use encryption technologies that will protect your private data from being accessed by others as you conduct an online transaction.
- Keep a record of your transactions. Just as you save store receipts, you should keep records of your online purchases. Back up your transaction by saving and/or printing the order confirmation.
- Review your monthly account statement thoroughly. Immediately investigate suspicious activity to prevent any possible additional fraud before it occurs. Promptly notify your financial institution of any suspicious email activities.
- Only open and respond to emails that pass some basic tests<sup>1</sup>, such as
  - o Is the email from somebody you know?
  - o Have you received emails from this sender before?
  - o Were you expecting email with an attachment from this sender?
  - o Does email from this sender with the contents described in the subject line and the name of the attachment make sense?
  - o Does this email contain a virus?

Should you receive any cardholder communication that you deem questionable, please contact us immediately at [CorpcomAP@visa.com](mailto:CorpcomAP@visa.com).

For more information on secure online shopping and how to manage your finances wisely, please visit [www.visa-asia.com/verified](http://www.visa-asia.com/verified) and [www.myMoneyskills.com](http://www.myMoneyskills.com)



<sup>1</sup>

Excerpt from "Common Sense Guide for Home and Individual Users", Internet Security Alliance, more information available from <[www.cert.org/homeusers/homecomputersecurity.html](http://www.cert.org/homeusers/homecomputersecurity.html)>