

## TIP #3:

# USE SAFE METHODS FOR PURCHASES

If you're going to make that purchase, what information are you handing over? Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.



If you can, **use a credit card as opposed to a debit card.** There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills.



**Check your credit card and bank statements for any fraudulent charges.** Immediately notify your bank or financial institution and local law enforcement.



**Be wary of emails requesting personal information.** Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email.



If you receive a suspicious email that you think may be a phishing scam, **you can report it at** <https://www.us-cert.gov/report-phishing>.

- If you believe your personal or financial information has been stolen, report it right away to your local police and the Federal Trade Commission (FTC). There's information on the FTC website, <https://www.identitytheft.gov/>, about how to report.
- Immediately change your passwords, use complex passwords, and use a different one for each account. A password manager can help you do this.

