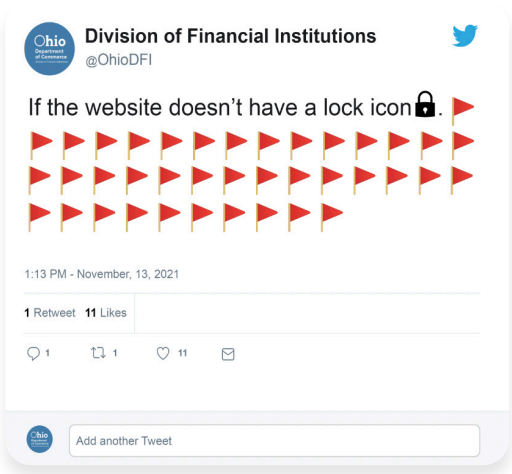
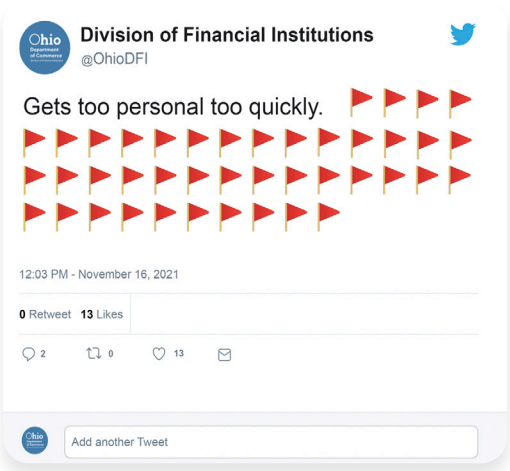
Online Shopping Dealbreakers That Could Land You on the Naughty List



Check the website security settings. If the site is secure, its URL (web address) should start with "https://" and include a **lock icon** on the purchase or shopping cart page. However, with scammers becoming more sophisticated, this should not be the only **red flag** you rely on.

Think before you click. Be especially cautious about **email solicitations and online ads** on social media sites. Many sketchy retailers advertise great deals or trendy clothing that don't measure up to the promotional hype. Not to mention, anyone can create an ad on social media platforms.

Protect your personal information. Read a site's **Privacy Policy** and understand what personal information is being requested and how it will be used. The most common location to find the Privacy Policy is in the footer of a website, and is grouped with similar items such as Contact Us and Terms and Conditions. This ensures the policy is visible for any visitors who wish to see how their personal data will be used.



Consumers who shop online with a credit card were less likely to lose money. Sites that ask for **payment in gift cards** is an automatic **red flag.** Be cautious when paying by peer-to-peer payment apps, prepaid money cards, or other non-traditional payment methods. Learn more about P2P apps and how to use each safely. Also, in case of a fraudulent transaction, a credit card provides additional protections; it's easier to dispute charges that you didn't approve or to get your money back if there is a problem. Debit cards, prepaid cards or gift cards don't have the same protections as a credit card.

Phishing attacks are a type of scam often used to steal user data, including login credentials and credit card numbers. Phishing emails or texts can look like a message from your financial institution or a mail carrier service but clicking on unfamiliar links can place you at risk for malware and/or identity theft. Don't be too quick to give out your personal information, scammers will try to push users into action by creating a sense of urgency. Be cautious with messages such as, "your account is locked" or "click this link for tracking updates" - don't take the bait!

Think you've been scammed?

- If you've been victimized by an online retail scam, file a report with the FTC and the FBI's Internet Crime Complaint Center. The FTC website also has advice on safe online shopping.
- Report fishy e-shopping operations to the BBB Scam Tracker, which also lets you search for scams in your region.
- File a complaint with the Ohio Attorney General.
- Contact your financial institution or creditor's fraud department and notify them of the situation.

Ohio Department of Commerce
Division of Financial Institutions