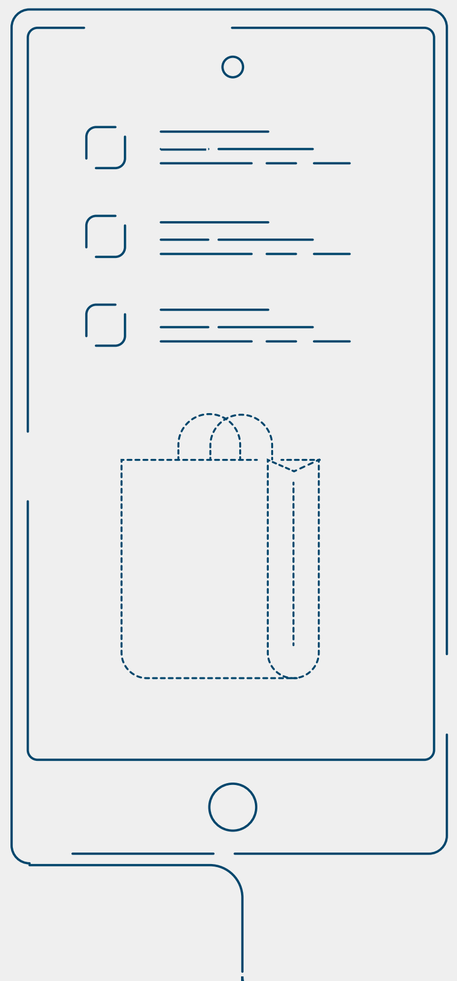
Global Learning Systems' cybersecurity checklist for online shopping



1

Don't click on links in emails, even if they seem to come from trusted retailers.

Instead, type the retailer's known URL dirrectly into your browser.

2

Don't do your holiday shopping on public Wi-Fi.

If hackers are using the same connection, they could see everything that you do.

3

Shop at trusted sites, and don't fall for ads from retailers you don't know.

Check for verified reviews, a physical address, and live support.

4

Vet mobile apps thoroughly.

Only download apps from major app stores, and ensure that you're getting the retailer's official app.

5

Lock your accounts.

Create a unique and long password for each account, for example: 1@mSmart&Happy! or !loveC0Okies&Cream.

6

Keep your credit card number private.

Don't save card info for your online accounts. Consider using a secure payment processor like PayPal or Apple Pay, or a virtual credit card (contact your bank for info).

7

Limit the personal information you provide.

Never share personal information such as Social Security Number. If a site asks for it, chances are they are not legit.

8

Check the site's security credentials.

Never buy anything from a site that doesn't have SSL (Secure Sockets Layer) encryption. It's not a guarantee, but a site without one is definitely insecure.

9

Check your credit card statement at least once a week for fraudulent charges.

A fake charge, even if it's very small, should be reported.

Global Learning Systems
Strengthen Your Human Firewall®