University Technology Services
University of South Carolina

# **Cyber-Shopping** Safely

E-commerce presents it's own unique challenges.

**Kyle S. Brown**

Kyle is an alumnus of the University of South Carolina and is currently the university's information security awareness specialist. He is part of the University Information Security Office where he works to help people understand the dangers of modern computing.

*Online shopping has become a popular way to purchase items without the hassles of traffic and crowds. But, the Internet can be risky. It is important to take steps to protect yourself when shopping online.*

## Secure your machine

Shopping safely on the Web begins with a safe workplace. In the context of this class, your workplace is your computer. If your machine is not safe, nothing you do on it will be either.

***At a bare minimum, the following needs to be done to have confidence in your computer:***

- Install, maintain, and use trusted anti-virus software.
- Turn on your system's firewall.
- Keep all software updated with the newest available version.

If you need help securing your computer, contact the UISO. Our office also teaches classes on how to get the most security out of Mac and PC platforms.

## What do you want, and where do you get it?

Now that you feel safe beginning a transaction on your machine, it's time to do some cyber-shopping! But, it is not time to get careless. There are some great deals to be found on the Web. There's also no shortage of bad ones.

Firstly, you should be the one doing the searching. You should never respond to **spam**, even if it offers the product of your dreams at a price that fits your budget. Most reputable companies will refrain from sending unsolicited messages. If the offer came to your inbox as **spam**, it could be fraudulent. These messages may be **phishing** attempts that try to trick you into providing your personal or financial information. Do not become a victim of ID theft.

## Due diligence

Now you've found the product you want, and likely several sellers who offer it at a resaonable price. Before beginning a transaction with anyone on the web, it's important to know who (and what) you're dealing with. Almost anyone can set up shop on the Internet, under any name. It's up to you to research vendors, sellers, and websites. This additional step will only provide you more protection.

***You should always look for:***

- Company information and contact info
- Feedback from other customers
- Merchant reviews
- Professional organizations - Are they a member of the BBB or similar club?

It is also important to research the product. Make sure the product description matches what you're buying.

UNIVERSITY OF SOUTH CAROLINA

## Making the Purchase

You've made it this far, now you're ready to close the deal. There are a few more things to look for before pulling the trigger.

### Where are you?

If you're sitting in your favorite coffee shop using the free Wi-Fi, you should probably wait. Unprotected networks can be easily scanned, allowing savvy eavesdroppers to intercept your information. No one wants a criminal knowing their name, address, phone number, or financial information!

It is best to make your purchase on a secured network. At a minimum, the network should require a username and password.

### What are you being asked?

Few things are more important than protecting your personal information. In today's world, data mining companies already know more about you than your closest relatives. There's no need to give them another advantage.

Cyber-criminals could also ask you questions to make it a bit easier to steal your identity, especially if you've been duped by a **phisher**. It is always important to remain alert to the kinds of information that is being collected to complete the transaction.

Always ask, "Do they need this information about me?" You should expect sellers to need payment information, names, and shipping addresses. If they start asking for your birthdate, SSN, or other private details, red flags should be flying high.

***You should read the privacy policy. It can help you understand why sellers want your data, and how they'll protect it.***

### Check Site Security.

You should never enter your personal or financial information on an unsecured site. Unsecured sites do not have an SSL certificate and most likely lack encryption. This means your information could be easily intercepted by a crook and could be used without your authorization. It always pays to look for signs that a site is secure.

There are a couple of easily recognizable signs that a site is secured. Firstly, somewhere in your browser's address bar, your should see the image of a small closed padlock. The lock is typically yellow, grey, or green and signifies to the user that the site is protecting your information.

Secondly, you should always check the URL itself. An unsecured site's URL will begin with "http://". If the URL begins with "https://", you are on a secure site. For our purposes, that "S" simply means secure. It really only indicates that the traffic is encrypted.

***http://amazon.com - unsecured***
***https://amazon.com - secured***

### How to pay.

Like in all transactions, eventually it comes time to pay the piper. You should remain vigilant during this part of the transaction. The methods of payment you choose could have an impact on your financial health beyond your purchase.

If a seller asks for payment via wire transfer or cash only, that is a good sign that it is time to walk away. Wire transfer and cash only scams are some of the most popular on the Net. These methods of payment can be difficult, often impossible to track during an investigation. You'll have no course of action if the transaction doesn't go as planned.

It is also wise to use a true credit card (with a low spending limit) for online purchases, rather than a bank-issued debit card. Credit cards allow buyers to seek a credit from the issuer if the product isn't delivered, or in some cases, if you're unsatisfied with the purchase. Credit cards generally have a limit on the monetary amount you'll be held responsible for if your information is stolen and used by someone else. If your debit card information is stolen and used, a crook could simply drain your accounts overnight. Banks are getting better at handling these situations, but it is a slow refund process.

## After the Purchase

Now that the purchase has been made, you need to maintain a paper trail (or an electronic trail). It's helpful to print or save records of your online transactions. Make sure you have the product description, price, receipt, terms of sale, and all communication with the seller. That way, if the product doesn't arrive as promised, you'll have plenty of records to fall back on.

We recommend you check your credit card (or bank) statement as soon as it arrives. You should verify that the item was charged appropriately. Further, examine the statement from the date of purchase to make sure you do not notice unauthorized charges. These may not look the same as the original transaction. If you see bizarre charges, like donations you don't recall, you should immediately notify your bank or card servicer immediately.

**If you're having trouble with a seller, it's always best to try to work it out with them directly. If that does not garner the desired results, most legitimate sales sites offer support and mediation. If all else fails, report online shopping fraud to the Federal Trade commission, South Carolina Attorney General, and South Carolina Consumer Protection Agency.**