Internet Safety Tips

Passwords - Your password is your prime defense against unauthorized access to your personal account. Do you want someone reading your e-mail or reviewing your banking records? Of course not, so it’s important to choose your passwords carefully and just as critical, to safeguard them.

- Don’t use passwords that consist of easily obtainable personal information, such as your address, phone number or date of birth. Also avoid using common words found in a dictionary.
- Devise passwords of at least six characters and consisting of upper and lower case letters, numbers, and symbols, for example: 2le@rN.
- Use a different password for each service you register with.
- Ideally, a password should be easy to remember. However, the reality is that having multiple passwords becomes confusing; which password is for which site? If you need to record your passwords, store them in a secure location. A piece of paper in the top drawer of your desk is tempting fate. Even worse is a Post-It note on your monitor!
- Never disclose your password.
- For sensitive accounts, such as financial services, change your passwords frequently.

E-Mail

Don’t mix business and leisure. Get an e-mail address for personal use.

You have little privacy protection with company e-mail. Most businesses claim that it is their right and responsibility to monitor e-mail because it represents the company, uses company equipment and travels over the company network. You could argue the point, but getting a private e-mail address is much easier. Use your business address for company business only.

Ignore spam.

- Sure, junk e-mail is a nuisance, but it’s easier to get rid of than the paper kind—just hit the Delete key. If you reply to spam, asking to be removed from the list, it just confirms that your address is valid. You will soon be spammed and spammed again.

Remove old e-mail from your computer.

- When you delete messages, they are still on your system. To permanently remove them, open the Deleted Mail folder, highlight the messages and delete them again. Some e-mail programs automatically empty deleted mail once you close the program.
- Be aware that messages may still reside somewhere on your computer. A trained technician may be able to recover them. Messages may also remain on the mail server and be archived in file back-ups.
Secure Site Transactions - Data is secured with a technology called encryption. Encryption software scrambles the data with a secret code so that no one can make sense of it while it's being transmitted. When the data reaches its destination, the same software unscrambles the information. When you see a small lock icon at the bottom of your web browser or next to the address bar, it indicates that your data is encrypted during transmission.

When dealing with online merchants, the best security is common sense. Anyone can establish a professional looking online store these days, so make sure you deal with reputable companies. How can you tell? The answers to these questions provides clues:

- Is this the website of an established retailer?
- Does the site have a street address, not just a post office box?
- Is there a way to call customer service?
- Is a return and refund policy posted?

All online financial transactions should be secure. Many online stores have what’s known as a secure check-out page. You may see a notice to that effect posted on the site. Alternately, you may see a lock icon on your web browser, indicating that the site uses security technology. Also, check the address of the web page in the address bar of your browser; it should begin with https. The letter "s" indicates that the page is secure.

If you are uncomfortable transmitting sensitive information, many sites provide a phone number you can call to give your credit card number, although there is no guarantee that's secure either. According to the National Consumers League, most Internet fraud involves sending checks or money orders to merchants. The organization recommends paying by credit card, because fraudulent charges can be disputed with your bank.

The risks involved in transacting business on the Internet are no greater than those in any other arena in which we do business. While it is relatively safe to conduct business on the Internet right now, there are many companies working to develop and improve the technology required to make the Web even more secure.

Almost everything you do online, whether it's visiting a website, reading a blog, downloading music or sending e-mail, leaves a trail of personal data. Some of it remains on your computer; some is transmitted to third parties. While this is not necessarily a bad thing, you can and should control who sees it. In the interest of protecting your privacy, we offer some tips.

Ten Tips for Smart and Safe Shopping

Reputable sites use technologies such as SSL (Secure Socket Layer) or SET (Secure Electronic Transmission) that encrypt data during transmission.

You can tell if this technology is in use when you see a lock icon in your web browser window. Another way is to check the address of the web page you are accessing; it should begin with "https". By the way, never send your credit card number by email!
Shop with businesses you already know and trust.

Many retailers now offer online shopping. One advantage is that some let you return merchandise to their stores, instead of shipping it back. If you want to make a purchase from a store you haven’t heard of before, do some research. Start with the Better Business Bureau Online. Also, make sure the site lists a physical address, not just a post office box. Finally, check to see if it displays seals from consumer protection organizations such as the previously mentioned Better Business Bureau Online and TRUSTe.

You can also see what other shoppers have to say about a particular merchant by checking reviews at Bizrate and Epinions.

Another option is doing a search with Google. Enter the name of the merchant along with the keyword "scam". You may discover some interesting results.

Look for coupons and other discounts.

Many online merchants offer rebates that can save you a bundle of money. To receive the discount, typically you enter the coupon code in the order form. It’s then deducted from the total purchase price. Start your bargain hunting at Learn the Net Coupons.

For travelers, many airline sites offer weekly specials and e-fares. To keep informed of these discounts, sign up for newsletters at their websites.

Comparison shop.

So-called shopping bots compare prices for products across dozens of websites. You’d be amazed at the range of prices. Start with these:

- PriceRunner
- PriceGrabber.com
- Shopzilla
- Smarter.com

Be skeptical.

Be wary of deals that appear too good to be true. They probably are. If you have suspicions, call the merchant and ask those tough questions. No phone number listed on the site? Then take your business somewhere else.

Check the shipping costs.

Shipping, especially for next day delivery, could make the total purchase price more than what you would pay in a retail store. At one time, many sites offered free shipping as a way to attract customers. While those days are over except during the holidays, some sites still offer free or discounted shipping for select items and purchases over a certain amount.
**Protect private information.**

All reputable sites should post a [privacy policy](#) that explains what they do with customer information. Take a few minutes to review it. If you don’t agree with the policy—some sites sell data to third parties—don’t shop at the site. Even if you have no objections, *don’t provide unnecessary information* by filling out the optional fields in the [order form](#).

**Review the return and refund policies.**

How can you return unwanted merchandise? How long do you have? Will you receive a full refund? Who pays for return shipping? An e-tailer should provide answers. If not, call the merchant before you buy.

**Pay with plastic.**

In the U.S., credit cards offer the same consumer protection whether shopping online or offline—you are liable only for US $50 if your card is used fraudulently. You can also challenge charges and withhold payment in the event of a dispute with a merchant.

An alternative payment option, particularly for buying from auction sites, is setting up an account with PayPal. You electronically transfer money from your bank account into your PayPal account, then use it to pay merchants.

**Print a copy of your order for your records.**

After you submit an order, you will get a screen with details of the transaction. Sometimes there is a link to a [web page](#) where you can check the delivery status. You may also receive an e-mail confirmation.

**Check here for more tips on keeping you and your children safe on the Internet**


**Check here to learn more about text slang**
