Internet Service

The Internet has changed the way we work, socialize and shop—we can now do all those things without ever leaving home. But that doesn't mean the Internet is always safe, or that it's always free. This fact sheet explains your options for Internet and email service. It also explains some risks of using the Internet and provides tips for protecting yourself, your family, and your personal information and computer data.

Internet service and email

- Internet service can be received by dial-up (via your household phone line), cable (via your cable television company), DSL (via phone company lines), satellite (via a "dish"), or wirelessly (wi-fi). Fiber optic broadband is not widely available yet.
- Dial-up is the slowest of the pay services. Faster types of Internet service often are referred to as "high-speed" or "broadband" Internet.
- Dial-up service can cost as little as $10 per month. DSL and cable prices typically fall between $35 and $65 per month, depending on provider and speed. Satellite and fiber optic service, if available, is more expensive. Promotions are available for new customers and for customers who bundle their service with phone and/or TV.
- Wireless Internet is available free in some locations (known as hotspots). Other locations (some hotels, for example) charge a fee. You may be able to get home wi-fi in conjunction with your cable modem or DSL service. Or, you may be able to buy wi-fi on its own, to use anywhere.
- There are more Internet service options in urban areas than in small towns or rural areas. Learn more at www.fcc.gov/cgb/consumerfacts/highspeedinternet.html.
- Email service is free, either through your Internet service provider (ISP) or a Web-based email service (Google's Gmail and Microsoft's Hotmail, for example).

Internet safety

- Adjust your social networking account settings for greater privacy, so that you share your information only with the people you choose, and not the general public.
- Monitor your children's Internet activity. Make clear what information is okay to share and what is not, and that it's never okay to meet a new online "friend" alone. Learn more about kids' online safety at http://kids.getnetwise.org.
- Report inappropriate, unwelcome or harassing communication to authorities, which may include police, your ISP, school officials and the FBI (www.ic3.gov).

Privacy of your personal information

- Secure your home wireless network with a strong password (at least eight characters long, consisting of upper and lowercase letters, numbers and symbols) and enable built-in encryption options.
- Use a firewall (built into newer computers), a virtual barrier between your computer and the Internet that all incoming and outgoing data must go through.
- Don't send sensitive data via email or instant messaging (IM) on any Web-enabled device. Be cautious when using publicly available wi-fi.
- If you use a public or shared computer, never save your login information, and always log out. Use the "in private" or "delete browsing history" feature of the browser, if available, to hide which sites you've visited.
- Reduce unwanted online marketing messages by revealing as little as possible about yourself at sites you visit. Don't open pop-up ads.

TURN OVER

- Read a site's privacy policy to learn how it will use your information. Look for logos, such as TRUSTe and BBBOnline, on the site.
- Shop only with reputable online merchants. Don't allow sites to save your credit card information for future purchases. Shop with a credit, rather than a debit, card.
- Before shopping on an unfamiliar site, research its complaint record. Then look for the SSL security encryption (https:// rather than "http://") in the address bar and a closed padlock or unbroken key in the window frame. Double-click the padlock or key—if the names in the Web address and on the security certificate don't match, the site may be bogus.
- A request for your Social Security number, username, password or other sensitive data indicates that an email may be "phishing" for your personal information to use fraudulently. If you question the authenticity of an email, do not reply. Forward it to your ISP and file a complaint with the Federal Trade Commission (FTC). Learn more or file your complaint at www.OnGuardOnline.gov.
- If you've already responded to a "phishing" email, immediately change the passwords on your accounts and notify the institution where you have the account. Review your credit reports (www.AnnualCreditReport.com) for signs of identity theft. You are entitled to receive three free credit reports a year.

Security of your computer data

- Viruses, worms, Trojans and spyware all are ways your computer data and personal information could be stolen, damaged or deleted. Always use antivirus software and antispyware, and update the software regularly to take advantage of protection against new threats. (Set up automatic updates, if possible.)
- Use your email service's spam filter. Delete (without opening) suspicious email that gets through the filter.
- Be careful about opening attachments or downloading free content from the Web—the files could contain a virus, spyware, or other malicious code.
- Malicious websites are designed to look like legitimate sites, but they attempt to steal your information or do harm to your computer and data. Never click links or visit pages sent by someone you don't know and trust.
- Don't forward chain letters. Check out questionable emails on anti-hoax sites (www.snopes.com or www.quatloos.com) before forwarding.
- Back up files regularly so you don't lose data. (Learn more at www.StaySafe.org.)
- Use special disk cleanup software or a tool in your operating system to fully delete all personal files before you get rid of your computer.

Handling disputes

- Avoid a dispute by knowing the terms of your service agreement.
- Broadband prices are based in part on download speeds. If you're not satisfied, test your own connection at http://www.broadband.gov. (Be aware that actual speeds depend on many factors, including your computer processor and Web traffic.)
- If given the option, opt out of an arbitration agreement—you don't want to give up your right to sue your service provider in court or join a class action lawsuit.
- Try to resolve your issue directly with your service provider within 30 days of receiving the bill. Keep track of all communications. Pay the undisputed portion of your bill by the due date. If you're not satisfied with the resolution, you can contact your local Better Business Bureau (www.bbb.org) and your local and state consumer protection agencies (http://consumeraction.gov/state.shtml). (The FCC does not regulate the Internet or ISPs.)

Consumer Action created the Empower U project under a grant from the California Consumer Protection Foundation. Consumer Action empowers low to moderate income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. To learn more, visit www.consumer-action.org.