Microsoft

4 Look for signs that a webpage is secure and legitimate

Before you enter sensitive data:

> Look for a web address with https ("s" stands for secure) and a closed padlock beside it. (The lock might also be in the lower right corner of the window.)

> Make sure you're at the correct site—for example, at your bank's website, not a fake. One sign of trustworthiness is a green address bar like the one above.

5 Save financial transactions for your home computer

Never pay bills, bank, shop, or do other financial business on a public computer, or any computer you don't manage, or on any device (such as a laptop or cell phone) over a public wireless network. The security is unreliable.

6 Use common sense

To protect yourself against fraud, watch out for These might appear as deals that sound too good to be true, alerts from your "bank" that your account will be closed unless you take immediate action, phone calls from a "relative" desperately needing money, or a refusal to meet in person for a local transaction.

Microsoft

More helpful info

> If you invest online (a topic not covered here), don't miss this U.S. government guidance about how to invest safely: **onguardonline.gov/topics/online-investing.aspx**.

> Find out more about phishing, and how to recognize and protect yourself from phishing scams: **aka.ms/phishing-FAQ**

> Look into consumer protection advice from the U.S. FDIC about safer online banking: **www.fdic.gov/bank/individual/online/safe.html**.

Making Safer Financial Transactions Online

Practical advice about banking, bill-paying, giving, shopping, and selling online

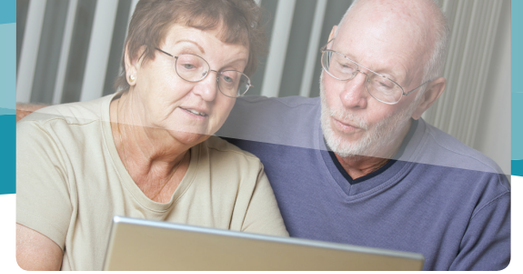
> Six basic rules for safer Internet transactions

> Safety tips for specific online transactions

> What to do if there are problems

1011 PN 098-111337

Microsoft



Six basic rules for safer Internet transactions

Whether you go online to check your bank balance, pay a bill, give money, shop, or sell something, these six rules can help you keep the risks to a minimum. For advice specific to each transaction, look inside.

1 Defend your computer

Help protect your online transactions by keeping all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Protect your wireless router with a password, and use flash drives cautiously. Microsoft can help: **microsoft.com/security/pypc.aspx**.

2 Create strong passwords

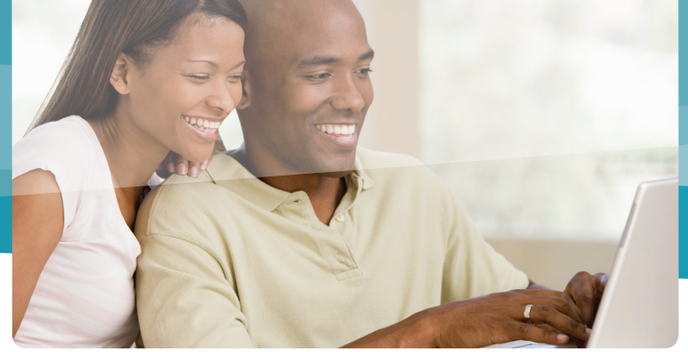
Strong passwords are easy for you to remember but difficult for others to guess. They are long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)

> Keep passwords and PINs secret. Don't share them in email or instant messages, on social sites, or over the phone.

> Use unique passwords for bank and other important accounts. Don't use the same password everywhere. If someone steals it, all the information it safeguards is at risk.

3 Find the web address yourself

Clicking a link in email, text, or instant messages or in a pop-up ad may land you on a site that looks legitimate, but isn't. To visit a website, type the address or use your own bookmark or favorite.



Safety tips for specific online transactions

Banking and paying bills

Monitor your account activity to help detect potential fraud by requesting credit reports. Every year, you're entitled to one free report from each of the major U.S. credit bureaus: Experian, Equifax, and TransUnion. Consider spacing these throughout the year.

The easiest way to get credit reports is by visiting **AnnualCreditReport.com** or by calling toll free: **(877) 322-8228**.

Stay alert to "phishing" scams

Typically these email, text, or instant messages, disguised to be from a reputable company, entice you to visit a phony website or call a fake number. There, criminals collect your financial data. (If in doubt, call the company.)

Learn to spot phishing scams and defend against them: **aka.ms/spot-that-scam**.

Shopping at online retailers and auction sites (like eBay) or making donations

Buy from reputable stores and sellers; give to legitimate charities. If you don't know them by reputation, find out what others say. Evaluate businesses at such sites as Epinions.com and BizRate.com, and charities at charitynavigator.org. Review buyer feedback about an auction seller, a key indicator of reliability.

Read the site's privacy policy to see if they resell your information.

Check the terms of the sale, such as shipping and handling fees, warranties, delivery dates, and refund and return policies (Only use sites that give full refunds.)

Give only enough information to make the purchase. Be wary if a merchant asks for bank account information, social security number, or other such data.

Choose a safer way to pay. Use a credit or charge card that offers cardholder protection, or a payment service like PayPal, which shields your credit card number from sellers. Never use debit or ATM cards, checks (even cashier's checks), money orders, or wire transfer services (such as Western Union or MoneyGram).

Be cautious about storing your password, address, and credit card data on sites (including for one-click shopping). Your info is only as secure as the methods used to protect it.

Print or save a copy of your order, including the confirmation number or email message, as your receipt. Verify payment yourself rather than follow links from the seller.

Buying and selling locally–online

Online classified sites like Craigslist, Kijiji, and Gumtree help you sell and buy things locally.

Limit personal information in your ad. Photos should not show other possessions, house details, or people. Only give a general location in the ad, not a specific address.

Only deal with someone you can meet in person. Out-of-area offers are almost always scams.

Inspect or show an item safely.

- If an item is portable, arrange to meet in a busy public place, not at your house or theirs.
- If you must go to a house or have someone come to yours (say, for a big item), be sure someone is always with you. Also, limit access in your home–some fake interest in items to scout a house for robbery.

Choose cash for in-person transactions. Checks give away personal information, putting you at risk.

- Don't use wire transfer services or accept money orders or cashier's checks (which can be bogus). Scammers favor these.
- If you're buying or selling a high-value item, think about going to the bank with the buyer or seller. If you consider an escrow service, check the classified site for its recommendation as some can be set up to commit fraud.
- Don't make or accept a partial payment with the promise of getting your item or remaining cash later.
- Be suspicious of offers to pay more than the asking price or requests for personal financial data to transfer funds to your account. Both are likely scams.

What to do If there are problems

Online shopping problem? First, ask the seller to make things right. If that doesn't work, contact the web service for help.

Report scams, fraud, identity theft, or other abuse:

- To the web service, local police, and the bank, credit card company, or other financial institution.
- For identity theft, to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft**, or call toll free: **(877) 438-4338**.
- For scams or fraud, to the FTC at **ftccomplaint assistant.gov**.