
# Help and consumer education

There are many things you can do to help protect yourself from fraud and keep your accounts and devices safe. A good place to start is with our top five security tips:

## TOP 5 TIPS

### 1 Always think, "This could happen to me."

Thinking this way will make you less likely to fall for attacks. You will protect your information, keep security measures in place and discover issues faster by keeping an eye on your accounts.

### 2 Be aware.

Be aware of people manipulating you for your information, sometimes called "social engineering." When a stranger calls or emails, you should treat him or her like a stranger.

- Only share information over the phone if you made the call to a number you know is right. Calls from numbers that look legitimate may be bad guys "spoofing" the incoming number to fool you.
- Use caution when sharing or verifying information.
- Only share your email address with people you know, and when you know how they will use it.
- Question or ignore people contacting you with wild offers or promises, like free money, in exchange for your information.

### 3 Know BEFORE you open.

Only open email and text messages from someone you know. Only open an attachment or click a link if you know and trust the sender, and you understand what the message is about.

- Read carefully to make sure you know the sender.
- Question or ignore any message asking for personal or financial information. (AT&T will never do this through email or text.)
- Do not provide your username or password through an email or text in response to an unsolicited email or text.

### 4 Strengthen your own security.

Be tough.

- Keep security software up to date.
- Keep all computers, laptops, tablets and mobile phones up to date with the latest operating system updates.
- Know the new guidelines for increasing password security:
  - Create unique passwords using a combination of random words or phrases, preferably longer.
  - Do more than simply change the number at the end of an existing password.
  - Avoid using nicknames, birthdays or other information people may know or is readily available, like information on your personal social media site.
- Use security questions with trick answers.
- Use two-step authentication where available. The first step is logging in with your password. This triggers the second step – a PIN number sent to your telephone that is required to complete the login.

### 5 Check it out.

Be your own private investigator.

- Look for security indicators on the website. These include an "s" after the http in a website address, and a lock icon at the bottom of the screen.
- If asked to fill out a form or share information, go directly to the company's secure website to submit the information. Don't fill out forms attached to emails or click on links in an unsolicited text message.
- Monitor your bank and credit card statements for suspicious charges or transfers.