

Before you walk away from a shared computer, make sure you haven't left anything behind!

Being able to access the Internet from a shared or public computer is a great convenience, but it can also pose a security risk to personal information. Here are a few things you need to remember.

1. Never leave the computer unattended while you're logged in.
2. Don't check the "remember my password" box.
3. When you're done, make sure you log off and close all applications
4. If possible, clear the browser cache and history.

It could be phishing if ...

- ✓ There are misspelled words in the e-mail or it contains poor grammar. Especially apparent if the phisher's first language is not English and the text was translated by a computer or website like BabelFish.
- ✓ The message asks for personally identifiable information, such as credit card numbers, account numbers, passwords, PINs or Social Security numbers.
- ✓ There are "threats" or alarming statements that create a sense of urgency. For example: "Your account will be locked until we hear from you" or "We have noticed activity on your account from a foreign IP address."
- ✓ The domain name in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact. For example: Phishing website: www.regionsbanking.com. Real website: www.regions.com.

Stay safe when buying or selling online.

Internet auction sites and online stores appear to make shopping a breeze, but buying or selling merchandise online can have risks. Visit the following sites to learn more about keeping your online accounts and personal information secure and how to guard against fraud.

PayPal Identity Protection

<https://www.paypal.com/idprotection?ssPageName=CMDV:AB>

eBay Security & Resolution Center

<http://pages.ebay.com/securitycenter/?ssPageName=CMDV:AB>