Gone are the days when you wait for the bank to mail a bank statement and you balance your account before you spend any more money. Many of us now rely on online banking on our computer, smart phone or tablet. We check our accounts often and rely on this to make financial decisions.

More than three million people used mobile banking last year, up 10 times over a year earlier. If you're not yet using your phone to check your balance, pay your bills or move money from account to account, you will soon.

But even though we rely on mobile banking to conduct our business, smart consumers ask the question, “How safe is it?” The biggest risk of mobile banking is also the reason it is so popular — mobile devices are easy to carry around everywhere we go. However, they also have everything from passwords to contact lists to our calendar appointments. Information like that can be dangerous if your mobile device falls into the wrong hands.

Consumers need to be more cautious than ever when banking through any device, as hackers can prey on the unsuspecting. Here are five tips on how to keep your identity safe and your money in the bank:

- Put a password on your phone or tablet so that only you can use your device. This will help protect you if your phone or tablet is ever lost or stolen. Some devices require you to trace a pattern or insert a PIN. While it might slow you down to have to enter a PIN each time you want to use your phone, this might be enough to keep a thief from accessing your bank account before you can report your phone as missing. Report lost or stolen devices immediately to your wireless provider and financial institutions.

- Public connections aren't very secure. In fact, most places that offer a public Wi-Fi hotspot warn users not to share sensitive information over the network. If you need to access your account information, you may want to switch to another
network. If you're using a smartphone or other cellular device, disabling the Wi-Fi and switching to a cellular network is a good solution. You never know who might be listening in over the public network.

- You should never follow a banking link sent to you in a text message or e-mail. “Phishing” refers to the practice of tricking someone into revealing private information. Fishing and phishing are similar concepts — there's bait involved with both. With a phishing scheme, that bait might be as simple as a text message or e-mail. Thieves have even been known to fake a website that is similar to the bank’s official site. Watch for anything that looks different on any website you visit regularly.

These fake links could potentially lead you to a spoofed website. If you enter your information into such a site, you've just handed that data over to thieves. If you’re not sure about a request, contact your bank by calling the number on the back of your debit or credit card.

It's always a good idea to navigate to a website directly. Enter your bank's web address into your phone and bookmark it. This will help you avoid bogus websites.

- Don’t stay logged into your accounts. Even though it’s convenient, it increases the risk that an unauthorized user will access your accounts.

- Delete old texts from your bank.

I’m not saying you should not use your mobile device to access your bank accounts. Just be sure to practice good, safe behaviors and keep track of your gadgets. With careful attention, mobile banking can be both convenient and secure.

**Roxie Rodgers Dinstel is a professor of extension on the Tanana District Extension Faculty. Questions or column requests can be e-mailed to her at rrdinstel@alaska.edu or by calling 907-474-2426. The Cooperative Extension Service is part of the University of Alaska Fairbanks, working in cooperation with the U.S. Department of Agriculture.**

- 30 -