DOs and DON'Ts to Beat Identity Theft and Protect Your Financial Security

Your personal information is at risk every time you write it down or post it online. It's critically important for your financial security that you take some simple steps to secure your information.

The week of March 4-10 is National Consumer Protection Week. Opportunity Bank of Montana (Member FDIC) is taking this opportunity to remind customers that it employs sophisticated safeguards and imposes strict policies to protect customer information. Nonetheless, customers call the bank every day to report that someone has accessed their personal information and used it to steal money, says Mandy Allen, bank officer and vice president for BSA, fraud, information & physical security.

Here are some measures Allen recommends that you can take to thwart costly identity theft:

1. DON'T open (most) email or text attachments

That is, don’t open them unless you are sure of the sender’s identity and the purpose of the attachment. You should never download an EXE, SCR or BAT file, which can take control of your computer or phone, unless you have asked for it.

2. DO use a passcode lock on your phone and tablet

This adds an extra layer of security on your personal devices.

3. DO install virus and malware protection on your phone

Just as you do with your home computer, particularly if you conduct business over your phone.

4. DO use a password manager

That allows you to access all your passwords with a single umbrella password that you can remember without storing on your computer or mobile devices.

5. DON’T keep your phone logged into a mobile banking session

Left open, the app can be accessed if someone steals or finds your phone.

6. DON’T allow anyone to “shoulder surf”

Opportunity Bank recently dealt with a case of a customer whose information was stolen by someone looking over their shoulder while they entered it into the phone.

7. DO avoid public WiFi hotspots when using passwords or personal information

Allen recommends that you never use the WiFi in public libraries, hotels, or even – gasp! – coffee shops if you’re entering sensitive information. “It’s easy for a hacker to spoof the hotspot address and then you’re just entering in information for them to steal,” she said.

8. DO join the Do Not Call registry

You can join the national Do Not Call registry at donotcall.gov or 888-382-1222. Allen also recommends opting out of pre-screened credit offers by visiting OptOutPreScreen.com or calling 888-567-8688.

9. DO shred documents regularly

Your credit card account number is on your credit card bills. Your bank account number is on your bank statement. Thieves still mine people's garbage for information they can use to make money. Buy a shredder – and use it.

10. DO use common sense when emailing and taking phone calls

Banks, the IRS and most reputable companies have policies against sending personal information via email or calling and asking for it. Don't share information on these platforms. When customers call Opportunity Bank, "we ask out-of-wallet questions that typically a fraudster wouldn't know, like the name of the joint owner of the account or the amount of their direct deposit and where it comes from," says Allen.

11. DON'T wait to report any issues to your bank

If you suspect fraud, nip it in the bud. And if you lose your phone or change your phone number, contact your bank immediately.

Identity theft is so lucrative and prevalent these days, so it's especially important that consumers play a role in the security of our own information. Opportunity Bank reminds you that National Consumer Protection Week, celebrated March 4-10, is really every week of the year.

For more information about Opportunity Bank and how they're keeping customers safe, visit OpportunityBank.com or stop by one of the nearby branches.

Suggested Social Media posts:

Facebook: 11 steps you can take to secure your personal information. [LINK]

Twitter: 11 steps you can take to secure your personal information. #consumerprotectionweek [LINK]

Facebook: Opportunity Bank marks National Consumer Protection Week with tips to protect you. [LINK]

Twitter: Opportunity Bank marks #NationalConsumerProtectionWeek with tips to protect you. [LINK]

Facebook: Did you know not to input personal information while on a public WiFi hotspot, like at the coffee shop?[LINK]

Twitter: Don’t input personal information while on a public WiFi hotspot, like at the coffee shop! #consumerprotectionweek [LINK]

Facebook: You know that anti-virus software on your computer? You need it on your phone too. [LINK]

Twitter: You know that anti-virus software on your computer? You need it on your phone too. #consumerprotectionweek [LINK]