Getting Social With Your Bank

➥ Some tips for using financial institutions' social networking sites

Getting Social With Your Bank

Many people connect with friends, meet new people and interact with businesses on "social media" sites such as Facebook, Google+ and Twitter. Banks are also using social media to advertise their products and services, obtain feedback from consumers, and, in some cases, provide a gateway for customers to access their accounts. Financial institutions also often use social media to share information with their local communities and to solicit feedback from them.

Should you consider using social media to connect with your bank? And, if you do, what should you keep in mind? Before you decide, you should visit your bank or its Web site to learn about its social media policies. You can learn how the bank is using social media, its guidelines, and other ways to communicate and conduct your banking business.

Advertising Products and Services

"There can be benefits to using social media to interact with banks," said Elizabeth Khalil, a Senior Policy Analyst in the FDIC's Division of Depositor and Consumer Protection. "You might find out about new bank products or services more quickly or be eligible to obtain special offers. You might also obtain faster responses to your questions or complaints."

And in December of 2013, federal regulators including the FDIC issued guidance reminding banks that the

laws that apply to institutions' activities in general continue to apply when they use social media. For example, when a bank uses Facebook to advertise loans, the bank must provide accurate disclosures just as it would in a newspaper advertisement.

Communicating With Your Bank

If you want to communicate with your bank on Twitter or Facebook, keep in mind that your posts could become public, even though you can protect your tweets and Facebook posts to some extent through your account settings. You should not include any personal, confidential or account information in your posts. "Also, reputable social media sites will not ask you for your Social Security, credit card or debit card numbers, or your bank account passwords," said FDIC Counsel Richard Schwartz.

Before posting information such as photos, comments and links, you should look for a link that says "privacy" or "policies" to find out what can be shared by the bank

"Also, reputable social media sites will not ask you for your Social Security, credit card or debit card numbers, or your bank account passwords,"

or the social media site with other parties, including companies that want to send you marketing e-mails. Read what the policies say about whether, and how, personal information will be kept secure. Also find out what options you may have to limit the sharing of your information.

"Look carefully to see whose site you are on and which policies apply," Khalil said. "You might have started out on the bank's page, but clicked on a link that took you to another company's page, where that company's policies will apply."

It is also best to avoid posting personal information that a fraudster could use to impersonate you. Information that may seem innocuous to share could be helpful to an identity thief. "Be cautious, even with details such as the name of your pet or a school you attended," advised Schwartz. "That type of information is often requested by banks for their security 'challenge questions' that are used to control access to accounts. A fraudster could use that information to log in to your account."

"Social media is inherently conversational and somewhat informal. That can lull people into a false sense of security, making them less careful with their personal information than they otherwise might be."

Khalil said that some social media sites require or encourage people to provide their birthdate. "You should evaluate how comfortable you are providing this and similar information and who, if anyone, would be able to see it," she suggested. Also, she added, "Social media is inherently conversational and somewhat informal. That can lull people into a false sense of security, making them less careful with their personal information than they otherwise might be."

Banking Through Social Media

Some banks use their social media sites as a portal for consumers to bank online. Anyone interested in doing so should first determine whether the page is really the bank's page or if it appears to be fraudulent.

Make sure you are on a secure page — and on the bank's legitimate site — before you enter your username, account number, or password. Some fraudsters have become sophisticated at mimicking official Web sites.

Look for clues that might indicate that the site is fraudulent, such as misspellings or a low number of "likes" on a page. If only a few consumers are subscribed to a social media page that supposedly belongs to a very large bank, that could be an indication that the page you are on is not the bank's official page.

You should also look for a padlock symbol on your Web browser. If you have any doubts, go directly to your bank's Web site instead of linking to it from a social media site.

Resources

To learn more about online activities, including the importance of using a security/anti-virus software program for your computer or phone and keeping it updated, there are many good resources from the federal government. One is the FDIC's Web page "Safe Internet Banking" at www.fdic.gov/bank/individual/online/safe.html.

In addition, the Federal Trade Commission at www.ftc.gov/bcp/menus/consumer/tech.shtm has good information, especially the "OnGuardOnline" site on using the Internet safely. You can also call the FTC toll-free at 1-877-382-4357.