



By: Laura Wainman--Elon University

## **Locked-Down Online: Safety and your online accounts**

In today's Twitter-paced society, paying bills by mail and depositing checks at the local branch doesn't cut it. Most of us go online to manage our financial accounts. It's more convenient, more efficient, and more flexible. However, that doesn't mean it's risk-free to perform sensitive transactions on the Internet. The good news is that financial institutions and government agencies are catching on to criminals that try to take advantage of the system.

### **Federal requirements**

In October 2005, the Federal Financial Institutions Examination Council issued a guidance to all financial institutions, suggesting that multifactor authentication controls should be used to verify the identity of customers. Essentially, these controls are additional steps beyond the basic username/password level. These steps vary between financial institutions; examples include security questions created by the customer or a single-use-only password. Though it may add a few seconds to the experience, it's designed to protect your accounts. It's a blessing, not a curse.

### **Phishing**

A favorite way to get your info online is phishing. This is when thieves use spam or pop-up messages to trick you into giving up personal or financial information.

- Do not reply to or click on any links in spam email that ask you to confirm or update account information. Legitimate companies don't use email to obtain this info. If you have any concerns about your account, call your financial institution directly.
- Don't be fooled by threats of dire consequences if you don't respond to an email or message. This is merely a scare tactic.

### **Staying in the clear**

No matter what direction criminals approach you from, there are things you can do to make their goal harder to reach.

- Avoid public computers or unsecured wireless networks (like your local coffee shop). Online criminals can troll public networks. Someone with a little know-how can snatch your data (account numbers, usernames, passwords, etc.) right out of the air.
- Never enter any personal information on a website that does not have a padlock in the browser window or "https://" at the start of the web address.

These symbols mean that the connection between your computer and the website is secure. This isn't a foolproof indicator (icons can be forged), but it's a good start.

- Install anti-virus software on your computer before managing any accounts online. Criminals can extract personal information using malware and spyware.

For more information, visit your financial institution's website and review the section regarding safe online banking practices. When it comes to protecting yourself online, taking extra precautions is always your best bet.

**Bottom Line:** More than half of those between 18 and 34 preferred to manage financial accounts online in 2008. There will always be people looking for an opportunity to access your financial information. Be careful when managing your money online.

### **Stats**

Almost 20% of consumers that have experienced a data breach (when personal info is compromised) suffered some kind of fraud, according to an October 2009 report.

*Source:* [javelinstrategy.com](http://javelinstrategy.com)

There were \$100 million in attempted losses from phishing at small and medium sized businesses as of October 2009.

*Source:* [ic3.gov](http://ic3.gov)

brass|MEDIA Inc. licensed content is provided with the understanding that the publisher, copyright holder and organizations distributing the magazine are not rendering investment, financial or other professional advice. Investment and other financial decisions depend on each reader's individual facts and circumstances. You should not make decisions based on information contained in licensed brass content without the advice of a qualified professional.