9/23/16

By Susan Grant, Consumer Federation of America Director of Consumer Protection and Privacy

The news that at least half a billion Yahoo accounts have been affected by a data breach –and that the company took two years to publicly acknowledge this – is very distressing, and not only to Yahoo users. It makes us wonder if we can ever rely on anyone who has our personal information to keep it safe. It's not just businesses that suffer from data breaches. The running list of breaches maintained by the Identity Theft Resource Center includes government agencies, schools, and healthcare providers. In Yahoo's case, while the passwords that were stolen were encrypted, it does not appear that other information that may have been compromised, such as customers' names, email addresses, telephone numbers, dates of birth, and security questions and answers, was protected by encryption. The company says that unencrypted passwords, payment card data and bank account information were not involved in the breach. It may seem like closing the barn door after the horse has escaped, but Yahoo users should still take these precautions:

Change your Yahoo password. And if you use the same password on other accounts, change those, too.

Change your Yahoo security questions. And it you use the same questions on other accounts, ditto.

Consider using two-factor authentication to access your Yahoo account. This provides an extra layer of security by requiring you to enter a one-time code, which will be sent to you by text or phone call, during the log-in process. Go to https://help.yahoo.com/kb/activate-sign-in-verification-sln5013.html .

Watch out for phishing attempts. Don’t click on links or download attachments in emails that appear to be from Yahoo – they could be from crooks trying to trick you into providing even more personal information or enabling them to get into your computer. And be wary of calls or texts asking for your personal information. Yahoo doesn’t need it, it already has it.

Monitor your accounts for suspicious activity. This is especially easy to do if you access your accounts online, but you should also look at bank and credit card statements and bills that you get in the mail to see if there are any charges you never made.

Place a fraud alert on your credit report and get a free copy. Fortunately no financial information appears to have been stolen, but by piecing together bits of information it might be possible for crooks to open new accounts in your name, so it’s wise to take steps to make that harder to do, and it’s free. Go to
identitytheft.gov
for information about this and other things you can do to reduce the possible damage from this breach.