Cyber-Attacks

Cyber-terrorism tactics…and how they could affect you

Safety and security remain your bank's chief goal

Cyber-attacks against the U.S. financial system are very much in the news lately, with attacks coming sometimes several times a week. These cyber-attacks are the focus of concern for both government and industry, as experts seek ways to identify the perpetrators and stop the attacks.

As a bank customer, it is important for you to know the facts about these events, so you can interpret the news and decide for yourself how these attacks might affect you and your finances.

The key facts to remember:

- Financial institutions on a regular basis evaluate their security systems to better protect against the threat of cyber-attacks.
- Security system evaluations include: business resilience, authentication, system configuration, security tools, data protection and employee training.

Here is additional information about the cyber-attackers, their methods, and their results:

■ What is a cyber-attack?

Cyber-attacks on banks most often take the form of distributed denial of service attacks (DDOS). These "denial of service" attacks flood a target organization's website with traffic. Attackers focus on one or two pages—such as the Welcome page or Log In page—hitting it a much as 20 million times a minute. This causes the system to operate slowly as it sorts out the difference between honest requests for service (such as a customer's), or requests that carry viruses and malware that attempt to cause harm (such as a hacker's). The purpose of the cyber-attack is to keep the bank's security system busy, sometimes denying customers online access to their accounts.

How long should I expect to wait?

Attacks have been known to last up to six hours or more. As the system sorts out the dangerous requests, you might have to wait longer than normal for service. During this time, you may wish to use one of your bank's many other avenues to access your financial information, such as mobile, ATM, phone, or branch access.

Who are these cyber-attackers?

Government and industry experts know that the technology required for such massive Internet hacking cannot be accomplished by a typical basement hacker. Rather, governments, presumably countries unfriendly to the US, have the resources to back operations of this sophistication and expense, according to US government experts.

What can I do to protect myself?

Continuing to use the same common sense security tactics as always is still your best defense. Tips are included here to refresh your memory.

- **Strong passwords**—Experts advise a combination of letters (some capitalized), numbers, and symbols at least ten characters in length. And advise against using easily guessed passwords such as birthdays or home addresses.
- **Multi-factor authentication**—A method of logon verification where at least two different factors of proof are required to allow an individual secure account access.
- **Anti-virus protections**—Make sure the anti-virus software on your computer is current and scans your email as it is received.
- **Email safety**—Email is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way.
- **Sign off and log out**—Always log off by following the bank's secured area exit procedures.
- **Monitor your accounts**—When you check your accounts regularly, you can let your bank know immediately if you encounter anything that does not seem right.

Crooks are always trying to get your personal information, and they employ some ingenious methods. Don't respond to any unusual email requests for personal information—when you opened your bank accounts you already gave it.

When in doubt, call your bank.

Resources

- Internet Crime Complaint Center
  www.ic3.gov
- Federal Trade Commission
  www.ftc.gov
- Financial Fraud Enforcement Task Force
  www.stopfraud.gov
- Identity Theft Resource Center
  www.idtheftcenter.org