CYBER-ATTACKS

Cyber-Terrorism Tactics… and How They Could Affect *You*

Safety & 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 are

- ☑ **Your personal information is safe**
- ☑ **Your money is safe.**

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

What Is a Cyber-Attack?

Cyber-attacks on banks 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 as 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), and a request that might cause harm (such as a hacker's). The purpose of the cyber-attack is to keep the bank's security system busy, thus denying customers access to their accounts.

So It Only Slows the System Down?

That is the extent of the recent attacks. As the system sorts out the dangerous requests from the others, you might have to wait longer than normal for service. With 20 million requests from the cyber-attackers and one from you, it's not hard to understand why!

How Long Should I Expect to Wait?

Attacks have been known to last up to several hours. 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 on-site service.

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 is still your best defense. Tips are included here to refresh your memory.

- ✔ **Strong Passwords**—Experts advise a combination of letters and numbers, and advise against using easily guessed passwords such as birthdays or home addresses.
- ✔ **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.

Resources

- **Internet Crime Complaint Center:** www.ic3.gov
- **Consumer Fraud (Department of Justice Homepage):** www.usdoj.gov
- **Federal Trade Commission (FTC) Consumer Response Center:** www.ftc.gov
- **Consumer Guides and Protection:** www.usa.gov
- **Financial Fraud Enforcement Task Force:** www.stopfraud.gov
- **On Guard Online:** www.onguardonline.gov