



E-mail Banking Scams

From the Office of Minnesota Attorney General Lori Swanson

Online banking is becoming an increasingly popular banking option, due to the convenience that it may offer some consumers. Although online banking with a reputable bank is typically a secure practice, a new e-mail scam, targeted at individuals and businesses alike, may jeopardize the security of your financial account information.

How the Scam Works

Fraudulent actors send out mass emails to individuals, businesses and other organizations, claiming to represent their financial institutions. The e-mails generally indicate that the financial institution has experienced problems with their records, due to a security breach or computer system failure. The e-mail typically indicates that the recipient's financial account may be frozen if he/she does not act quickly in response to the e-mail by clicking on an internet link on the page. By clicking on the link, the recipient is navigated to an official-looking website which asks the individual to disclose their account information and other personal information, in order to "verify" their identity. Once the fraudulent actors have obtained the personal information, they are then able to make unauthorized withdrawals from the account in question, or apply for credit in the account-holders name. Individuals and businesses tricked into disclosing their information have reported losing large amounts of money in this scam.

There are several elements of this scam that may make it particularly troublesome. First, the fraudulent actors frequently counterfeit the logo of a reputable financial institution with an imposter version. Scam artists have copied the logos of well-known banks to trick customers of these financial institutions into disclosing their information. Since the logos are well-mimicked, the e-mails can trick even cautious consumers.

Second, the fraudulent actors use sophisticated tactics to cloak the URL of the website. The URL is the address of the webpage that appears at the top of most internet browsers. Although the false URL may indicate the page belongs to a financial institution, it actually belongs to a scam artist, who is often located outside of the United States.

Protect Your Account:

- 1) Beware of e-mail requests to "verify" your account information online. Your bank already knows your account number and does not need to verify it. Furthermore, in the event of a security breach or computer problem, most banks contact their customers in writing or by telephone to discuss the matter.
- 2) Contact your financial institution through trusted channels. If you are concerned about receiving such an e-mail, call your bank immediately at the publicly-listed phone number.
- 3) Don't be rushed by suspicious e-mails. Since many individuals, businesses and non-profits rely on the financial viability of their account in a given day, the prospect of a temporarily frozen account and lost business that could result can be particularly worrisome. Remember, however that the amount of money lost to such a scam is typically a much larger problem. Take your time to think logically and contact your financial institution directly.
- 4) Use a URL-checker. Computer users may wish to access software which allows them to check the accuracy of a given URL. This will help you know who you are dealing with online.

Concerns about Internet Scams?

Contact the following agencies:

Federal Bureau of Investigation

Minneapolis Office
111 Washington Avenue South, Suite 1100
Minneapolis, MN 55401
(612) 376-3200

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
Toll free: 1-877-382-4357

United States Secret Service

Minneapolis Field Office
300 S. 4th St., Suite 750
Minneapolis, MN 55415
(612) 348-1800

For more information about identity theft contact:

Office of Minnesota Attorney General

Lori Swanson

Consumer Services
1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101
(651) 296-3353 or 1-800-657-3787
www.ag.state.mn.us

