



With the security of Visa,
you can stay in control of
your financial and personal
information online.



Learn the Latest Online Security Measures

Follow these easy e-mail security tips...

✓ **Use caution with e-mails requesting information.**

Fraudulent e-mail often uses threatening language about freezing or terminating your account. Don't fall for this trick. Never provide your personal, financial, or account information in response to an e-mail request.

✓ **If you're not sure, don't click on the links.**

By clicking on false links you may launch a virus that will track your keystrokes. Instead, type the web address you want to visit into the browser address bar. If the e-mail is suspicious and no web address is provided, do not interact with the e-mail.



✓ **Check Alabama Credit Union statements regularly.**

If you receive a paper statement in the mail, check it right away. If you have online access, check your account more frequently. Report any suspicious transactions immediately.

✓ **Contact Alabama Credit Union.**

If you think that an e-mail is suspicious, don't respond to it. Instead, verify that the e-mail is genuine by typing the Alabama Credit Union website address, www.AlabamaCU.com, into your browser address bar or by calling the phone number shown on your Alabama Credit Union statement.

© 2005 Visa U.S.A. Inc, V13357-02-05c



Control. Protection. Confidence.

The security of Visa.

Visa® won't ask you to send personal information via e-mail.

Many businesses use e-mail to communicate with customers, direct them to their website, and ask them to enter personal information to log-in or register for a legitimate service.

Visa or Alabama Credit Union however, would never ask you to send your Social Security number, account number, password, or PIN to them via e-mail.



How to identify possible e-mail scams.

Posing as legitimate businesses, such as a financial institution, credit card company, Internet service provider or retailer, criminals send "official-looking" e-mail or set up websites to trick you into providing your personal or financial information. This illegal activity is called "phishing." Beware of any e-mail urgently asking you for:

- Credit card account numbers
- Checking account information
- Account passwords
- Social Security number

While online banking and shopping are very safe, be extremely careful about sending any personal or financial information over the Internet.

You're in control at all times.

E-mail scams often use scare tactics, such as a fake account problem or fraud warning, to get your attention. Or they may say that your account will be terminated or suspended if you don't respond. Either way, they're trying to convince you to give them your personal information. Don't do it.

Contact Visa if you receive an unfamiliar e-mail referencing Visa or Alabama Credit Union.

If you receive a suspicious e-mail, forward it immediately to phishing@visa.com or to your financial institution.

For more information on e-mail and Internet security, visit these websites:

- Visa: www.visa.com/phishing
- www.AlabamaCU.com
- Better Business Bureau: www.bbbonline.org
- Call for Action: www.callforaction.org.

See reverse for helpful tips.

