Colleen Tressler, Consumer Education Specialist, FTC, is reporting on scammers who are trying to take advantage of the millions of consumers who have not yet received a chip card.

**How Is It Happening?**
Scammers are emailing people, posing as their card issuer. The scammers claim that in order to issue a new chip card, you need to update your account by confirming some personal information or clicking on a link to continue the process.

**What Happens?**
If you reply to the email with personal information, the scammer can use it to commit identity theft. If you click on the link, you may unknowingly install malware on your device. Malware programs can cause your device to crash, monitor your online activity, send spam, steal personal information and commit fraud.

**What to Do?**
So how can you tell if the email is from a scammer?
- There is no reason your card issuer needs to contact you by email — or by phone, for that matter — to confirm personal information before sending you a new chip card. Do not respond to an email or phone call that asks you to provide your card number. Period.

- Still not sure if the email is a scam? Contact your card issuers using the phone numbers on your cards.

- Do not trust links in emails. Only provide personal information through a company’s website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the “s” stands for secure).

**More Information**
To learn more about protecting your personal information, check out the Federal Trade Commission’s web site: [http://www.consumer.ftc.gov/topics/privacy-identity](http://www.consumer.ftc.gov/topics/privacy-identity)