## Phishing, pharming, vishing and smishing

### Phishing

On the Internet, "phishing" refers to criminal activity that attempts to fraudulently obtain sensitive information. There are several ways a scam artist will try to obtain sensitive information such as your social security number, driver's license, credit card information, or bank account information.

**Here are some questions to ask if you think you have received a phishing attack:**

1. Do you know the sender of the email? If yes, still be cautious before clicking a link. If no, do not click any links.
2. Are there any attachments in the email? If so, is the attachment an executable (a file with the extension .exe, .bat, .com, .vbs, .reg, .msi, .pif, .pl, .php)? If so, do not click on the attachment. Even if the file does not contain one of the above mentioned extensions, be cautious about opening it. Contact the sender to verify its contents.
3. Does the email request personal information? If so, do not reply.
4. Does the email contain grammatical errors? If so, be suspicious.
5. If you have a relationship with the company, are they addressing you by name?
6. Have you checked the link? Mouse over the link and check the URL. Does it look legitimate or does it look like it will take you to a different Web site?

You can use these same questions if you receive a vishing or smishing attack.

### Pharming

Pharming is another scam where a hacker installs malicious code on a personal computer or server. This code then redirects clicks you make on a Web site to another fraudulent Web site without your consent or knowledge. To avoid pharming, follow the basic computer safety guidelines. Also, be careful when entering financial information on a Web site. Look for the key or lock symbol at the bottom of the browser. If the Web site looks different than when you last visited, be suspicious and don’t click unless you are absolutely certain the site is safe.

### Vishing

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Criminals also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on “social engineering” techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to pretend to be you and open new lines of credit.

To avoid being fooled by a vishing attempt:

- If you receive an email or phone call asking you to call and you suspect it might be a fraudulent request, look up the organization’s customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Though vishing and its relative, phishing, are troublesome crimes and sometimes hard to identify, there are things that you can do to protect your identity.

**Smishing**

Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again just like phishing, the smishing message usually asks for your immediate attention.

In many cases, the smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the SMS message was sent via email to the cell phone, and not sent from another cell phone.

Do not respond to smishing messages.