

## Phishing

Using email to leverage your trust in a company, brand, or person and trick you into providing personal financial information or access vehicles (passwords, account names, email addresses) to an unknown person or group.

If you receive an email that you think is a “phish”, the tips below can keep you from taking the bait.

## Receiving the Email

- 1. Know thyself:** Know the online companies you deal with. When a suspect email arrives, remember: it could be fraud, it's definitely spam, and it is definitely not for you. Delete it.
- 2. Subject matters:** Consider the subject line of an email carefully. Citibank will never send you an email headed “\_Citiibank\_account\_update ACT-NOW”. These messages may get through spam filters because they appear to come from a reputable source, but that doesn't mean it's really from Citibank.

## Looking at the Email

- 3. Learn the language:** Understand how the companies you deal with want to interact with you. For example, banks usually want you to access your account through their website—not an email link. “Phishing” emails stand out because they don't follow the rules.
- 4. Browsing around:** Practice safe browsing. Open a new browser window each time you log on to a web site that displays personal information. When you are done at that site, log out and close that browser window.
- 5. Spelling counts:** Be sure to read emails that say they are from companies you know. Sometimes a real email will have a spelling or grammatical error, but anything more than one error is suspicious.
- 6. Mousing around:** Scroll over the links in emails you receive and check them. In some email systems, you can scroll over the different links in an email and see the actual contents of the link. If the email says PayPal, but the link content says “ www.paipall.com”, be careful. And note: URLs can be disguised—so don't take a suspect link at face value.
- 7. All form, no function:** Never enter your personal or credit information into a form in an email. If you feel the email is legitimate, call the company or visit their web site and log in to provide the requested information.
- 8. It's personal:** Expect good customer service. Unless your name is “eBay User” or “johndoe99”, most “phishing” emails are not personalized. If you receive a “Dear Customer” email, it may be time to move on.

## Stay on Guard

- 9. Make a statement:** Read your statements – every one, every month to ensure your charges and debits are correct. Often information obtained through phishing is not used right away. Stay vigilant and report any suspicious activity immediately.
- 10. Stay current:** Use and maintain your email protection software for spam blocking, fraud blocking, and anti-virus. If you have any questions, there are many fine web sites which can provide the latest information on the latest virus, “phishing” attack, or on-line scam.

“Phishing” schemes will continue to get more sophisticated and harder to detect. A combination of technology and consumer awareness is the key to keeping the “phish” at bay and making your email good again.