Additional Information on Fraudulent Emails or "Phish"

What Is Phish?

Phish is email that appears to be from a legitimate business like Marriott, but is actually a scam to get access to your personal or financial information and commit identity theft. Older, less sophisticated versions of phish typically asked you to submit information by email. A newer approach is to direct you to a Web page that looks legitimate and ask you to log in, so that the "phishers" can get your user name and password and use them to access the rest of your information.

How to Identify Phish

Phish often displays one or more of the following characteristics:

- Asks for personal or financial information (e.g., credit card number, social security number, user name and/or password).
- Conveys a sense of urgency (e.g., "your account will be deactivated if you don't...").
- May have a lot of spelling or grammar errors.
- Looks like the logo and/or company name were just pasted into the email.

What to Do

If you receive an email that looks like phish, we recommend that you do the following:

- Forward the email to the Federal Trade Commission at spam@uce.gov or call 1-877-FTC-HELP (1-877-382-4357) to report it. The FTC uses the spam stored in this database to pursue law enforcement actions against people who send deceptive email.
- Delete the email.

If you believe "phishers" have gotten access to your personal or financial information, we recommend that you also do the following:

- Change your password.
- Contact credit reporting services ↗ and have a fraud alert attached to your credit report file. Please be aware that the perpetrator may attempt to use your information to establish accounts or obtain credit at other businesses in their name.

Additional Information on How to Protect Your Personal Information

- Anti-phishing working group ↗
- FTC Identity Theft Site ↗
- FTC guide on how not to get hooked by a phishing scam ↗