FEDERAL TRADE COMMISSION
Consumer Information
consumer.ftc.gov

Phishing: Don’t take the bait

March 6, 2019
by Colleen Tressler
Consumer Education Specialist, FTC

Phishing is when someone uses fake emails or texts – even phone calls – to get you to share valuable personal information, like account numbers, Social Security numbers, or your login IDs and passwords. Scammers use this information to steal your money, your identity (consumer.ftc.gov/articles/0005-identity-theft), or both. They may also try to get access to your computer or network. If you click on a link in one of these emails or texts, they can install ransomware (consumer.ftc.gov/blog/2016/11/how-defend-against-ransomware) or other programs (consumer.ftc.gov/articles/0011-malware) that lock you out of your data and let them steal your personal information.

Scammers often use familiar company names or pretend to be someone you know. They pressure you to act now – or something bad will happen.

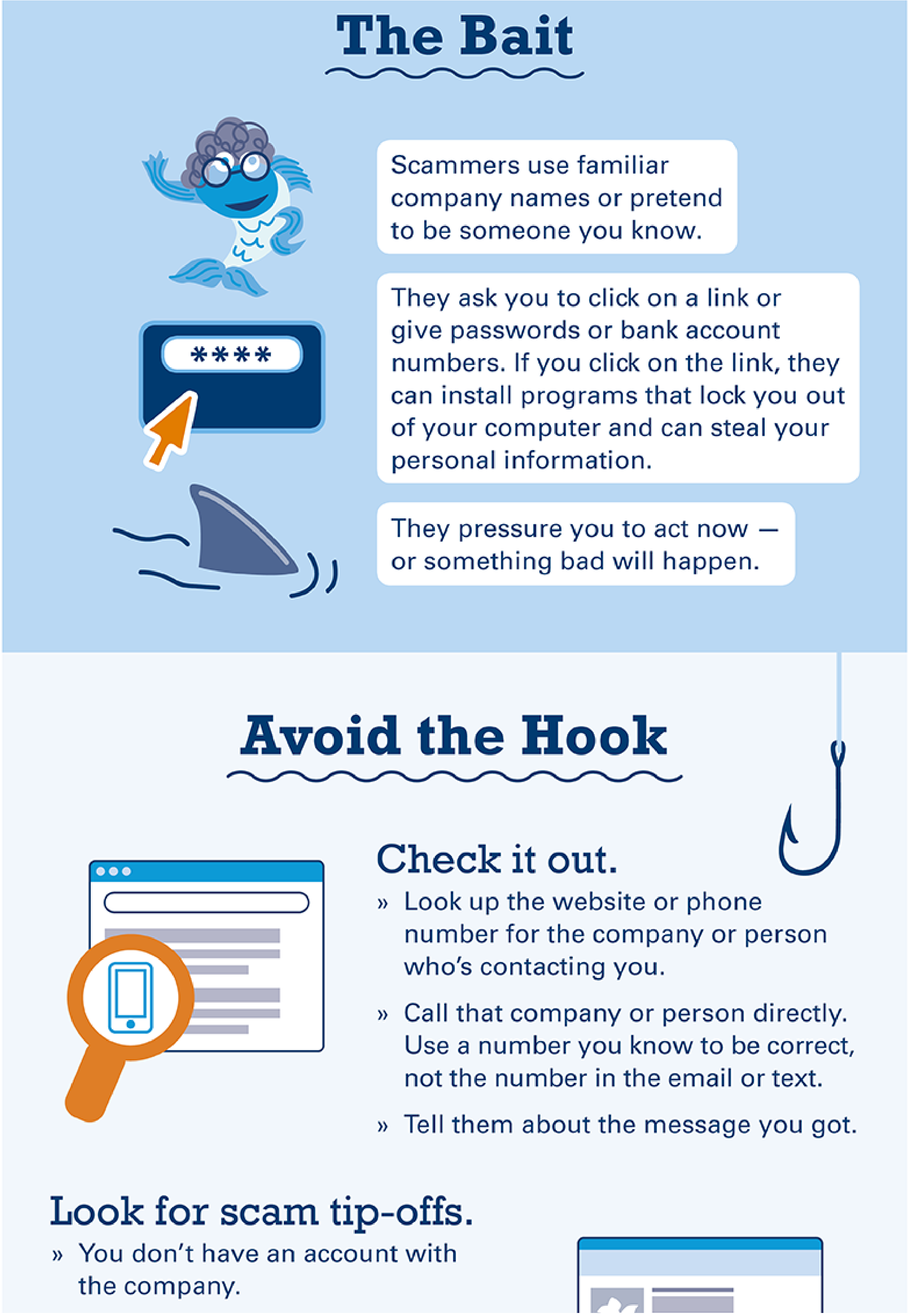
The FTC’s new infographic (consumer.ftc.gov/articles/phishing-dont-take-bait), developed with the American Bankers Association Foundation, offers tips to help you recognize the bait, avoid the hook, and report phishing scams.

Please share this information with your school or family, friends and co-workers. You can also test your knowledge by playing this al-luring game (consumer.ftc.gov/media/game-0011-phishing-scams).

Want to avoid the latest rip-offs? Sign up for free consumer alerts from the FTC at ftc.gov/subscribe (ftc.gov/stay-connected).

Phishing: Don’t Take the Bait

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they’re actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.



The Bait

Scammers use familiar company names or pretend to be someone you know.

They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.

They pressure you to act now — or something bad will happen.

Avoid the Hook

Check it out.

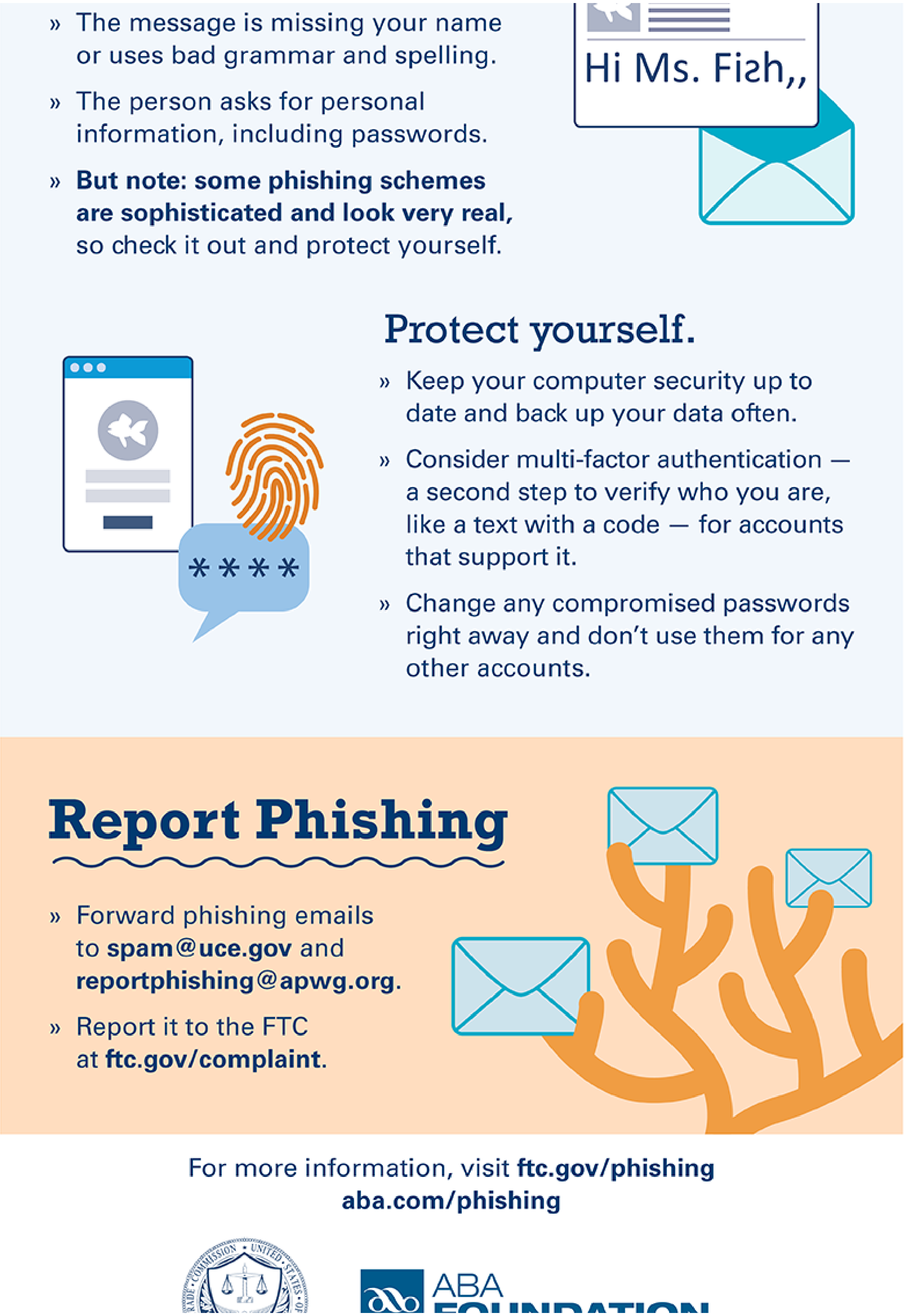
» Look up the website or phone number for the company or person who’s contacting you.

» Call that company or person directly. Use a number you know to be correct, not the number in the email or text.

» Tell them about the message you got.

Look for scam tip-offs.

» You don’t have an account with the company.



- The message is missing your name or uses bad grammar and spelling.
- The person asks for personal information, including passwords.
- **But note: some phishing schemes are sophisticated and look very real,** so check it out and protect yourself.

Protect yourself.

- Keep your computer security up to date and back up your data often.
- Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.
- Change any compromised passwords right away and don’t use them for any other accounts.

Report Phishing

- Forward phishing emails to **spam@uce.gov** and **reportphishing@apwg.org**.
- Report it to the FTC at **ftc.gov/complaint**.

For more information, visit **ftc.gov/phishing**
aba.com/phishing

ABA FOUNDATION

(consumer.ftc.gov/articles/phishing-dont-take-bait)

Blog Topics: Privacy, Identity & Online Security (consumer.ftc.gov/blog/privacy%2C-identity-%26-online-security)