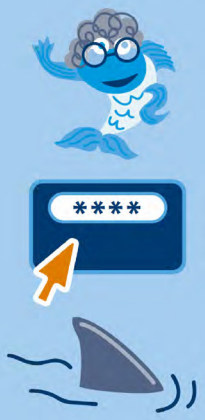
Phishing: Don't Take the Bait

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.

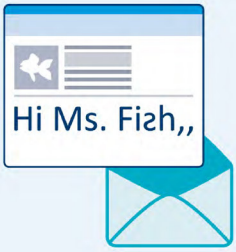
Avoid the Hook

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

- Report it to the FTC at **ftc.gov/complaint**.

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

ABA FOUNDATION

FAKE CHECK SCAMS

Did someone send you a check and ask you to send some money back?

MAYBE:

- You win a prize and are told to send back taxes and fees.
- You get paid as a "secret shopper" and are told to wire back money.
- You sold an item online and the buyer overpays.

IN ALL CASES:

You get a check.

They ask you to send back money.

THAT'S A SCAM.

IF IT'S A FAKE CHECK, WHY IS MONEY IN YOUR ACCOUNT?

Banks have to make deposited funds available quickly. It's the law. But the bank may not learn for days that the check was bad. By then, the scammer has your money. And you have to repay the bank. Remember — just because the check has cleared does not mean it is good.

WHAT TO DO:

- Be wary. Talk to someone you trust and contact your bank before you act.
- Never take a check for more than your selling price.
- Selling online? Consider using an escrow or online payment service.
- Never send money back to someone who sent you a check.
- Spot this scam? Tell the Federal Trade Commission: ftc.gov/complaint

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

ABA FOUNDATION