Recognizing phishing phone calls and emails

<h2><p>Be suspicious of any unusual request for your personal or financial information by email or phone. It may be a “spoof” or “phishing” attempt.</p>

</h2>

<h2><h3>The easiest way to identify whether an email is from us is to check your eBay Messages. If we sent the message, a copy of it will appear there too.</h3>

</h2>

<h2>
If you believe your account is compromised, see our page on getting help with a hacked account
For information about gift card fraud, see our article on protecting yourself against gift card scams
Scammers may impersonate well-known companies via email, phone, or text message in the hope that recipients will provide confidential information (including passwords or bank or credit card details) and/or download malicious software.If a message demands you take immediate action, includes attachments or links, asks you for personal information, or promises a deal that is too good to be true, you should be cautious. This may include a request for wire transfers to overseas accounts, the purchase of prepaid cards, or cryptocurrency. Don’t click on links that come from people you don’t know, and don’t respond.<h2 id="section1">Phishing phone calls</h2>eBay is unlikely to make unannounced calls to you about your account.If you receive a missed call from someone purporting to be from eBay, do not call the number back.If you’re unsure whether the request was genuine or not, check your eBay Messages - opens in new window or tab as we will have also sent you an

email.<h2 id="section2">Email phishing attempts</h2>A phishing email pretending to be from eBay typically contains a link that takes you to a fake website. There, you’ll be asked to sign in and submit personal and account information.These emails often include the eBay logo and a fake eBay address in the “From” line.Here are some typical traits of phishing scams:
Asking for confidential information
An urgent or threatening tone that asks you to act quickly
Unsolicited attachments
A generic greeting, like “Attention eBay member”
A web address that looks like eBay, but which may have a typo or extra numbers and letters (like http://signin-ebay.com or http://signin.ebay.com@10.19.32.4)
<h2 id="section3">Report a phishing phone call or email </h2>If you receive a suspicious phone call or email, you should report it to us immediately. Here’s how:Suspicious phone call
Tell the caller that you’ll call back through official eBay contact channels. If you missed the call, do not call the number back.
Email us at spoof@ebay.com with details of what the caller asked for and the phone number they called from. Suspicious email
Don’t click any links in the email or open any attachments.
Forward the message to us as an attachment at spoof@ebay.com.
We’ll let you know that we received the email. Additionally, you should report the suspicious phone call or email to the Federal Trade Commission (FTC) - opens in new window or tab.<h2 id="section4">Recognizing legitimate contacts from eBay</h2>If we need to contact you about your account, you can expect the following:
We’ll never ask you to provide confidential information like your password or credit card details
We’ll only include links for convenience. No link will require you to

submit confidential information on the next page
We won’t include attachments. If you receive an unsolicited email with an attachment, don’t open it
We’ll never use threatening language
We’ll always send a copy of any important messages to your eBay Messages - opens in new window or tab
</h2>

<h2>eBay spoof email,eBay spoof email address,eBay phishing email,eBay spam email</h2>