

Account safety

GUIDE.SUMMARY What General account safety on eBay involves:

- Account information security
- Password security
- How to protect account information
- Personal email security

When Account safety is a priority at all times. During the transaction period, possible security issues may emerge in particular areas, including:

- Buyer transaction
- Spoof sites
- Username as bidder protection
- Seller communications
- Off-site transactions
- Seller transaction
- Confirmation of payment
- Confirmed shipping address
- Mule fraud

Who Account safety is a priority for eBay. Buyers and sellers have safety concerns about their account information and security. These include:

- Passwords
- Spoof sites posing as eBay / PayPal
- Confirmation of transactions

This article covers

- Talking points
- Keeping your account safe
- Changing passwords
- Recognizing fake sites
- Off-site purchases
- How eBay keeps your information safe
- "Mule scams"
- 2 Factor Authentication (2FA)
- Detailed information

When a member states or suspects unauthorized access

- SMS limits for 2FA

- Instructions/steps to resolve
- Adding/removing and signing in with 2FA
- Receiving invalid code error
- General troubleshooting for SMS and email issues

Buyer Workflow

- When member suspects unauthorized use of account

GUIDE.RELATED_LINKS Related Help Pages

- Protecting member privacy:

<http://pages.ebay.com/help/account/protecting-privacy.html>

- Passwords tutorial:

href="http://pics.ebaystatic.com/aw/pics/securityCenter/tutorial/Password/story.html"

target="_blank">http://pics.ebaystatic.com/aw/pics/securityCenter/tutorial/Password/story.html
 Reporting spoof emails:
 <a href="http://pages.ebay.com/help/account/questions/report-spoof-email.html"

target="_blank">http://pages.ebay.com/help/account/questions/report-spoof-email.html
 What to do when your account has been stolen:
 <a href="http://pages.ebay.com/help/confidence/isgw-account-theft-reporting.html"

target="_blank">http://pages.ebay.com/help/confidence/isgw-account-theft-reporting.html
 Phishing/spoof tutorial:
 <a href="http://pics.ebaystatic.com/aw/pics/securityCenter/tutorial/Spoof/story.html"

target="_blank">http://pics.ebaystatic.com/aw/pics/securityCenter/tutorial/Spoof/story.html
 Account protection tutorial:
 <a href="http://pages.ebay.com/help/tutorial/accountprotection/js_tutorial.html"

target="_blank">http://pages.ebay.com/help/tutorial/accountprotection/js_tutorial.html
 The federal governments website to help people be safe, secure and responsible online:
 <a href="http://OnGuardOnline.gov"

target="_blank">http://OnGuardOnline.gov
 Related articles <a href="https://cskb.qa.ebay.com/csKBapp/art?page=content&id=GUIDE1098"

target="_blank">Contact Verification (CV) for Phone/Chat/Email <a href="https://cskb.qa.ebay.com/csKBapp/art?page=content&id=GUIDE1098"

target="_blank">Hard Verification (HV) for Phone/Chat/Email </h2><h2>GUIDE.TALKING_POINTS How can I keep my account safe? Never share personal account

information with an unverified contact. Bear in mind that eBay never asks members to provide financial account numbers, passwords, or other sensitive information. Emails from eBay that request information will always be in My eBay messages. eBay doesn't require members to enter information on any page that can't be accessed from the eBay site directly. eBay won't include attachments. If you receive a message that seems to come from eBay and has an attachment, do not open the attachment. Internal Information To report suspicious member account behavior, SHATO refer the Usernames and information received. I'm concerned about my account security. What should I do? You can keep your eBay account safe by following these steps. How often should I change my password? It's a good idea to change your password every 30 to 60 days. How do I know if I'm on a fake sign-in page? You should check to ensure that the web address is a secure one. The web address (URL) for an eBay sign-in page will begin with https://signin.ebay.com/ See Spoofer emails - Possible email scam tactics and how to avoid them. Why does the site keep making me sign in? You may be asked to sign in multiple times to protect your identity and privacy. If you want to change a password, add a seller's account, or use Live Chat, you will be requested to sign in. You can cut down on the sign-in requests by selecting the "Keep me signed in for today" check box on the sign-in page. That way, you will stay signed in even if you disconnect from the Internet or close the browser. You should only check that box if you are not sharing your computer or using a public computer. Why did I receive an email notifying me of a new login from a new device? As part of keeping your account secure, we will notify you when a new device (phone, computer) has been used to access the site that had not been previously used. This

will help ensure that your logins are indeed yours. If you don't recognize the login, we recommend that you change your password. If you can't access your account at all, we will review your account to ensure that it hasn't been accessed without your permission. Why am I being asked for a verification code when I change my password? Your account security is very important to us. You may be asked to enter a verification code if your password has been identified as not secure enough. This extra security step helps prevent account takeovers, automated registrations and inappropriate use of eBay. Why am I being asked to verify through the eBay app when checking out or doing certain activities on my account? Your account security is very important to us. You may be asked to verify yourself through a notification on the eBay app. This extra security step helps prevent account takeovers, automated registrations and inappropriate use of eBay. Why am I being asked to enter a SMS code to be able to send a message? The phone verification process helps us protect our members from fraudsters and ultimately ensures the safety of our marketplace. How do I know if the email confirming that I won/ bought my item is from eBay? Tips on knowing if an email is really from eBay:

- We never ask the member to provide financial account numbers, passwords, or other sensitive information over email.
- Emails from eBay that request information will always be in eBay messages.
- We don't require you to enter information on a page that can't be accessed from the eBay site directly.
- We won't include attachments. If you receive a message that seems to come from eBay and has an attachment, do not open it.
- Spoof emails or emails you are suspicious of should be forwarded to <mailto:spoof@eBay.com> or <mailto:spoof@PayPal.com>.
- Please forward any email referring to the purchase of a vehicle to </car@eBay.com>.

See <https://cskb.qa.ebay.com/csxbapp/art?page=content&id=GUIDE1073>

Spoof emails - Possible email scam tactics and how to avoid them.

Internal Information

- Walk member through the process to check "My eBay" and "Purchase History" to confirm that they won an item. The member can also enter the item number in any page's search box and click Search to bring up the listing and check to see if the member is the winning buyer.
- If the member is not in a transaction, suggest that they use the Ask the seller a question link in the item's description to request information regarding an item.
- Remind member that all transactional communication should be via eBay messaging.
- If a member requests another member's contact information, you may provide it through a contact information swap. However, only provide this information if it is absolutely necessary and approved by your team lead or coach. See <https://cskb.qa.ebay.com/cskbapp/art?page=content&id=GUIDE1039> Contact Trading Partner for more information.

a member attempts to take the transaction off eBay, this is against eBay policy and the member will not have the eBay Money Back Guarantee should the transaction not work out.

A seller contacted me to see if I was interested in buying an item that didn't sell. How safe is this purchase? Unless this is a Second Chance Offer, this message is likely to have arrived through spam (unsolicited commercial messages) via email or chat. It's important to note that:

- Offers to sell listed items outside of the eBay site are not permitted.
- Offers of this nature are a potential fraud risk for both buyers and sellers and circumvent eBay's fees.
- Items purchased outside of eBay include those bought directly from a seller or through item listings that either ended without a winning bidder or didn't meet the reserve price. (This does not include Second Chance Offers, which will present to the member through eBay messages.)

Transactions that happen outside eBay are a bad idea for many reasons:

- They have a high risk of fraud.
- They are not covered by PayPal Buyer Protection.
- They are not covered by eBay Money Back Guarantee.
- They are not eligible for Feedback.

How can I avoid your eBay account information being sold for solicitation? We put great importance on

member privacy and, per the Privacy Policy, we don't sell or disclose your personal information for marketing purposes. We limit the disclosure of contact information to other eBay members. This transaction seems "too good to be true". How to know that the item / seller is legitimate:

- For any questions regarding the item, use the Ask the seller a question link in the item's description.
- Review seller feedback on previous buyer experiences.
- Carefully review description, shipping, returns policy and payment options on listing, including item location.
- Confirm eBay Money Back Guarantee policy available on item. (The item will indicate the logo and explanation of policy on item listing.)

I'm a new seller; how do I know that I've been paid?

- Sign in to your eBay account and go to My eBay > Sell > Sold and review sold item. If payment has successfully completed, the "\$" sign to the right of your item title will turn from the color gray to dark blue.
- Sign in to your PayPal account and go to History and select Payments Received. Your transaction will have a "Payment Status".
- If PayPal was not the payment method, check with your recipient payment source (merchant credit card service, for example) to verify payment completion.
- If a different payment method was used, you can change the item's payment status manually using the Actions drop-down menu.

- Sellers can select Mark as payment received.

Once you, as a seller, mark an item as payment received, the item shows as "Paid" in the buyer's My eBay.

How do I know eBay secures my personal and financial information? Rest assured that:

- eBay uses the industry-standard Secure Sockets Layer (SSL) method of encryption to make sure that sensitive information is secure.
- The data is stored separately on secure servers and encrypted when it's sent between computers.
- The information that you submit is unreadable, except to those who have a secret key.
- Your information remains confidential and cannot be retrieved by anyone other than eBay.

When I sign in to eBay, the page is a secure https web page. Why aren't the rest of eBay pages also https? eBay protects all pages that

involve sensitive information with authentication and authorization controls. All critical flows that involve sensitive data are delivered over SSL (https). This incorporates the login flows but also further critical flows like registration, payment and critical updates to users profiles. Additionally, eBay has deployed a myriad of proprietary technologies to detect and prevent attempts of account misuse. These technologies run behind the scenes to protect the users' accounts against any illegitimate access. We are continuously investing at large scale into the security of our site. This includes the further development of our technologies to identify and prevent attempts of account misuse as well as the expansion of SSL usage on our site. What is a "mule scam"? A fraudster posts one ad and will get multiple people to respond. The fraudster has people create accounts under their respective names, and using their PayPal accounts. Items are then listed by account owners, who can easily verify themselves and their items if and when they are blocked by eBay's verification process. It's difficult for us to detect fraud until something goes wrong since the fraudster's name or business is not noted anywhere on the accounts. The member is left holding the bag, and the fraudster cannot be tracked. See Spoon emails - Possible email scam tactics and how to avoid them. What is 2 factor authentication (2FA)? For talking points about 2FA and Trusted devices see GUIDE1769 - Two Factor Authentication (2FA)

<h2><h2>GUIDE.DETAILED_INFORMATION See Buyer Workflow for members who state or suspect that there has been unauthorized access to their eBay account. Members can keep their eBay account safe by following these steps: Protect account information: Using a password and secret questions that are difficult to guess. Check out eBay's password resource:
 <a

A different computer is used.

Personal information is changed.

Suggest that member adds a cell phone number to their account information.

Limits for 2FA SMS

There is a limit to the number of attempts a customer can use before they are blocked. See <https://cskb.qa.ebay.com/cskbapp/art?page=content&id=GUIDE1769#DetailedInformation>

GUIDE.INSTRUCTIONSSTEPS_TO_RESOLVE

Adding or removing 2FA

To add or remove 2FA see <https://cskb.qa.ebay.com/cskbapp/art?page=content&id=GUIDE1769#InstructionsStepstoResolve>

Receiving invalid code error

Ensure you leave your browser window open until the email code is received.

You should not leave the sign-in page, close or click back on the browser, otherwise the old code will be revoked and will fail with the error message.

General troubleshooting for SMS and email issues

15 minute code delivery window

Make sure you have entered the code within the 15 minutes window. The code is invalid after 15 minutes.

Email code

Check your spam folder. It is known that code emails sometimes are recognized as spam.

SMS/text message

Make sure you can receive SMS/text messages. Landline is not supported.

Are you using multiple SIM cards?

If you are using multiple SIM cards, make sure that the SIM settings are set to either SIM1 or SIM2, depending on which one the proper number is.

Does the SIM card support SMS/Text message functionality?

In some cases SIM cards do not support SMS/text messages. You'll need to check your contract and check back with your mobile provider.

Network type of

the mobile phone

- Make sure that you have the proper network type selected in the settings. Usually this should be "Automatic" and selecting from G3, G4 or G5.

Proper mobile reception

- It has been found that SMS/text messages can get lost in cases where there is no proper reception. Make sure you have proper reception before sending the code (basements or thick isolating walls can limit the reach of the phone signal).

System PIN verification in use

- It has been found that some users have set-up system PIN verification for known devices (Face ID, Fingerprint, Windows 10/11 PIN etc.). Make sure you use your system verification PIN to log in.

SMS encryption in use

- Apps like Signal or Treema can handle SMS for users. It has been found that some users do not receive our SMS when using apps like Signal or Treema.

##