Spoof emails/phone calls - Possible scam tactics and how to avoid them

<h2>GUIDE.SUMMARY What <ul> Spoof emails (also known as "hoax" or "phishing" emails) are deceptive emails sent as a form of fraud. They fake the appearance of emails from eBay or other popular websites or companies. Dealing with emails safely is an important part of keeping yourself protected online (see Account safety for more information). Occasionally, customers have reported receiving spoof phone calls a fraudster pretending to be calling from eBay in order to solicit account details. Who <ul> Spoof email can be sent to any member, and may come from any type of sender. Examples include the following: <ul> Fake sellers may target buyers / bidders about an item they want, such as by sending false Second Chance Offers. Fake buyers may contact sellers to attempt to pay with fraudulent funds or send them fake payment notice emails. Fraudsters may impersonate eBay via email or phone in an attempt to gather personal information.   How <ul> Fraudsters will obtain email addresses through various means, then send spoof emails asking members for their personal information. The intent is that unsuspecting recipients will reply or click a link in the email and provide sensitive information, such as a password or credit card number. With this information, fraudsters may steal money from the member, assume their identity, take over their account (i.e., ATO), etc. This article covers <ul> What a spoof email is. How to identify and prevent spoof emails. What a member can do after becoming a victim of a spoof email. Workflow to help verify if an email is a spoof. How an agent should handle a spoof message sent to eBay. Spoof phone calls / members enquiring whether a call they received was

legitimate, including situations that may be legitimate.   </h2><h2>GUIDE.RELATED_LINKS Related Help pages <ul> Reporting and Recognizing Spoof (Fake) Emails
 http://pages.ebay.com/help/account/questions/report-spoof-email.html
   Securing Your Account and Reporting Account Theft
 http://pages.ebay.com/help/account/securing-account.html
   Recognizing Spoof (fake) eBay Websites
 http://pages.ebay.com/help/account/recognizing-spoof.html
   Minimizing unwanted email
 http://pages.ebay.com/help/account/unwanted-email.html
   Privacy Policy Summary
 http://pages.ebay.com/help/account/privacy-summary.html
   Protecting Your Privacy
 http://pages.ebay.com/help/account/protecting-privacy.html
    Related CSKB articles <ul> INV - Abusive Members / No intent to facilitate the transaction   <a

href="https://cskb.qa.ebay.com/cskbapp/art?page=content&id=GUIDE1529" target="_parent">Off-eBay Sales   My Messages (or Messages)   Account safety   ATO Policy
 Checkout - resolving errors </h2><h2>GUIDE.TALKING_POINTS How do I know if the message is from eBay? The best way to check if it is a valid eBay message is to check if the message is also on your eBay account. Go to My eBay > My Messages, and filter your messages to only those sent from eBay. If the email is not located there, it is not from us. There are some other useful guidelines for knowing if an email came from eBay.   If the member doesn't have an eBay account associated with the email address where they received the email, see e2M workflow. What should I do with the suspicious email? Please forward the message as an attachment so that we can review it for possible fraud. Emails that claim to come from eBay should go to spoof@ebay.com. Emails specifically about motor vehicle transactions should go to <a

href="mailto:car@ebay.com">car@ebay.com   Do not respond or click on any links provided by such messages. Many spoof messages may indicate that action is needed right away in order to convince members to provide personal information. How to prevent spoof emails. Follow these useful tips for knowing if an email came from eBay. We can refer you to related eBay pages with lots of helpful information on spoof emails that can help you learn more about how to protect your account. Only communicate with other members, update your account information, and submit payments directly through eBay. Claims that you need to do any of these actions off eBay should not be trusted. What does eBay do to protect its members from spoof emails? The My Messages system can help distinguish spoof emails. All emails in My Messages are sent through the eBay email system, and therefore come from us. We safeguard bidders' Usernames on the bid history of auctions so they're not as easy for fraudsters to find. We prevent you from using email addresses that start with your eBay Username, which prevents third parties from guessing your email address. We work with law enforcement agencies to help prevent internet crime whenever possible. What to do if you have already responded to the spoof. Monitor your account for suspicious activity. Your account may have been compromised. If you entered your password through an email, or feel that you may have signed in through a link that wasn't on the eBay site, change your password immediately. If you entered any credit card or banking information through a suspicious link, or through email, contact your bank or credit card company. Why cant you help me get my money back (already fell for the spoof)? Even though

they may be using our logo and claiming to be from eBay, these are in no way associated with us, and we cannot follow through on any promises made in those messages. We recommend that you contact the authorities to see how they can help. Contact the company you made the payment through to see if you can cancel or dispute the payment. Contact the police, both where you live and (if you know this) where the other party lives. Let the officers know that eBay is happy to cooperate in the investigation. The officer can find more information and contact us from our Law Enforcement page: <a href="http://pages2.ebay.com/Law_enforcement">http://pages2.ebay.com/Law_enforcement   Helping consumers/members when no money has been sent <ul> Please do not send any money. Scammers are using eBay's name to defraud consumers on non-eBay classified ad sites. Any listing that you initially found on Craigslist, Auto Trader, Cars.com or any other site where a seller promises eBay purchase protection is misleading and is a scam. If you received an email that appears to be from eBay, you may see terms like invoice, case id, transaction id, or VPP numbers. These are fraudulent tactics utilized by people trying to mislead you and steal your money. The only purchases that qualify for eBay purchase protection are those made on www.ebay.com where you have purchased the item with your registered account. eBay Vehicle Purchase Protection is only available for vehicles purchased on eBayMotors.com Other common fraud techniques include: the seller won't meet you face to face, the seller is selling due to military deployments, divorce or death in the family. If the deal is too good to be true, it probably is. Be on guard if you have never actually seen the item in person. These sellers will tell you to pay and that eBay will hold the money and pay you back if you are not satisfied. eBay will never hold your money for any reason or ask you to pay with any type of gift card, pre-paid card, Western Union or MoneyGram. If you would like you register for an account on eBay I can help get you started. Helping consumers/members when money has

been sent It will be important that you focus on the steps and give the consumer/member the information quickly and not drag out the conversation. Time is of the essence. Since you've sent payment, there are a few steps I'd recommend you take as soon as possible. Show empathy while you educate the consumer/customer. I am glad you called in and we certainly want to help you as much as we can I can hear how upset you are. Tell me what's going on. I share your concerns about this problem and respect all of the time and effort to solve it. I want to make sure we respect all your time and efforts you have put into this.   Find out how they paid. Direct them to contact the payment provider immediately as the payment provider may be able to help stop the payment or use of gift card codes. Rule of thumb for law enforcement <ul> Have them contact local police to report the fraud. If they received a spoof email, please have them forward it as an attachment to spoof@ebay.com. These emails are used as information when authorities contact eBay. About transferring calls to motors <ul> Please do not transfer the call to the Motors team if the subject is about a scam. Only Vehicle Purchase Protection calls should go to the Motors group. You have these talking points to help address when a consumer/member has sent money or not. The Motors team cannot do anything "special" for the customer. They speak to the same talking points as you would. You should never promise a customer that the motors team can recoup back money or gift cards sent to the fraudster. Please see the Transfer Guide for CS Phones, Chat and Email for any further questions about transferring spoof contacts.   </h2><h2>GUIDE.TIPS_FOR_MEMBERS Below are some useful guidelines on how to distinguish spoof messages/contacts from genuine eBay messages.

eBay messages will never: <ul> Ask you to provide financial account numbers, passwords or other sensitive information via email (emails from eBay that request information will always be in My Messages). Require you to enter information on a page that can't be accessed from the eBay site directly. Include attachments. If you get a message that seems to come from eBay and has an attachment, don't open it. Refer to you without your Username and full registered name. Spoof messages/contacts may include: <ul> eBay terms, department names, and often the eBay logo. A generic greeting like "Attention eBay Member". A forged eBay address in the "From" line, such as support@ebay.com. Just because the sender line includes @ebay.com does not guarantee the email is from eBay. Threats of account suspension or call for quick action. The subject may be something like "problem with your account". Requests to provide personal information or verify passwords. Links to web pages that look like eBay sign-in pages. Links such as: http://signin.ebay.com@10.19.32.4/ or http://signin-ebay.com/ asking the member to sign in. The eBay home page URL starts https://signin.ebay.com/ Choose your Username, eBay password and secret question carefully. You need to choose both a Username and a password that aren't related to your email address or any of your other online accounts. Using the same sign-in information for several online accounts means that if someone can access one of your accounts, they can access all of your other accounts. Creating a unique Username also reduces the amount of unwelcome email you might get from other eBay members. If your Username is the same, or

similar to your email address, you should change your Username. eBay users can contact you after you have changed your Username by using the Contact an eBay Member feature. Review the following Creating and Protecting Your Password page for tips on how to select a secure password: http://pages.ebay.com/help/account/create-password.html Note: You should change your eBay password every 30 to 60 days. In addition to changing your password regularly, you also need to change the secret question and answer associated with your eBay account. Beware of spoof email and websites requesting sensitive information. A major threat to the security of your eBay account is fake email and associated websites, called spoof email and spoof websites. You might also see these called phishing emails and phishing websites. Both are used to get your personal and account information. If you get an e-mail that looks like it's from eBay and mentions a problem with your account or requests personal information, and it's not in My Messages in My eBay, it's a fake email. Forward suspicious e-mails as an attachment to spoof@ebay.com eBay will never ask you to provide sign-in passwords, credit card numbers, or other sensitive information through email. If eBay requests information, we always direct you back to the eBay site. Review the following Reporting Spoof Emails and Recognising Spoof (Fake) eBay websites page so that you know what to do to protect your eBay account against these threats: http://pages.ebay.com/help/account/recognizing-spoof.html Install and update online protection software. Anti-virus software - Computer viruses can log and record keystrokes. Emails can have viruses that can find and send information from your files. Install the latest version of anti-virus software and use it regularly to scan your computer. Spyware protection - Spyware is software that is downloaded onto your computer without your knowledge to

collect personal information and record your Internet usage. By keeping your spyware protection up to date, you can make sure that people who want to steal your account or your identity won't have access to your computer. Internet firewalls - Firewalls are hardware or software that control the flow of information to and from your computer. Using a firewall helps prevent unauthorised parties from gaining access to sensitive information stored on your computer. It's especially important to use a firewall if you have a high-speed connection that is always connected to the Internet. Monitor your account for suspicious activity. Periodically check your My eBay account and preferences to ensure that no one has taken over or tampered with your account. It's a good idea to check all your online accounts, not just your eBay account. If you see anything out of the ordinary with your eBay account, report it to eBay immediately and act quickly to secure your eBay account and protect yourself from identity theft.   </h2>