Digital Safety Awareness

Share this answer

Digital Safety Awareness

Fraud Information & Awareness

Consumers are frequently targeted by criminals using reputable brands to compromise sensitive information. To help protect customers, we are providing the following fraud prevention information.

Safety Tips

- If you're unsure if a phone call or email is really from the company it claims to be, call the number from their legitimate website. Do not call the number that initially called you or one provided in the email.
- Look closely at the sender's email address and embedded URL's. More sophisticated scammers will create fake domains and websites that look nearly identical to the legitimate business.
- Hover your mouse over a link to see the embedded URL. Do not click on the link if the address is different than the display text.
- Be suspicious of unsolicited emails, phone calls, or text messages asking for personal or financial information.
- Never respond to emails or texts from someone you don't know or whose identity you can't confirm.
- Never provide personal or financial information unless you are certain of the identity of the person or business that is contacting you.
- Never open suspicious attachments or links.
- Never send money or other type of monetary payment to someone you don't know.
- Do not deposit a check that is sent to you with instructions to wire money back to the sender or a 3rd party. Banks are required by law to make deposited check funds available within days and identifying a fake check can take several weeks. If a check you deposit turns out to be fraudulent, you will be responsible for paying the bank back.
- Regularly monitor your financial statements to detect any fraudulent charges. If an unauthorized charge is made to your account, immediately contact your bank or account provider.

Common Email Scams

Phishing Emails

Phishing emails attempt to entice you to click on a link that will take you to a fraudulent website that may seem legitimate. The site may ask you to "login" with your user ID and password so the scammer can then use your login credentials to take over your real account. You may also be asked to input personal or financial information that could expose you to future compromises, financial losses, and/or

identity theft. The website could also contain malicious code or the email itself may have an attachment that installs malware on your device.

Phishing emails may use Ace Hardware's name and/or logo to make it appear legitimate.

Reward for Completing a Survey

These phishing emails claim they will send a free gift in exchange for completing a survey. Once the survey is completed, you will be asked to provide payment information for shipping and handling. Upon doing so, your payment information will be compromised by the fraud subjects. Ace Hardware will never ask customers for payment information as part of any survey or promotion.

If you receive a phishing survey email report it to fraud@acehardware.com and delete the email. Please be sure to include the phishing email as an attachment when reporting fraud.

Free Gift Card or Prize Giveaway

These phishing emails claim they are offering a free gift as part of a giveaway. Ace Hardware does not offer these types of promotions and we do not contact our customers through unsolicited email campaigns.

Order Confirmation

You will only receive an order confirmation email if you completed an order on AceHardware.com. If you did not place an order, the email is a scam; the perpetrators are expecting you to be concerned and click on a link in the email without considering its legitimacy. If you would like to see if an order was placed using your account, sign in directly using the Ace Hardware App or go to AceHardware.com.

Gift Card Scams

Ace Hardware gift cards can only be used at Ace Hardware stores and on AceHardware.com and cannot be used to purchase other prepaid or specialty gift cards. No legitimate government entity, including the IRS, Treasury Department, FBI, or local police department, will accept any form of gift cards as payment. Do not search your gift card balance within search engines. Only check your balance at https://acehardware.wgiftcard.com/rbc/acehardware or on the Ace Hardware mobile app.

Under no circumstances should you provide a gift card number and PIN over the phone or email to an unknown person. The unknown person may try to trick you into buying gift cards and giving them the cards' account numbers and PINs, which they may then try to use without your knowledge. Never share gift card account numbers or PINs from the back of the card with someone you don't know.

Common Gift Card Scams

IRS/Government Scam

Scammers call and claim that they are the Internal Revenue Service (IRS), Social Security Administration (SSA) or another government agency and that the victim owes that agency money. Sometimes the scammers say that the victim will lose their house or will be arrested if they don't pay immediately. The scammers then instruct the victims to purchase gift cards and give them the gift card numbers over the phone.

If you owe federal taxes, or think you might owe taxes, hang up and call the IRS at 1-800-829-1040. IRS workers can help you with your payment questions.

If you don't owe taxes, call and report the incident to the Treasury Inspector General for Tax Administration at 1-800-366-4484.

You can also file a complaint with the Federal Trade Commission at ftc.gov. Add "IRS Telephone Scam" to the comments in your complaint.

Tech Support Scam

Perpetrators of tech support scams try to trick victims into believing their computers are infected and they need help. Some scammers pretend to be associated with Microsoft, Apple or a familiar security software company such as Norton or McAfee and claim to have detected malware that poses an imminent threat to the person's computer. Such scammers will often ask for remote access to your computer to run phony diagnostic tests and pretend to discover defects in need of fixing. They'll pressure you to pay for unnecessary repairs or new software and ask for payment via gift cards.

SMS (Text Message) Phishing

Like its email-based counterpart, text message phishing (usually referred to as SMS (Short Message System) phishing or "smishing") uses social engineering tactics to gain access to private information. It may also use Ace Hardware's name or logo to make it appear legitimate.

Free Gift Card or Prize

Messages of this nature claim they are offering a free prize as part of a giveaway. Ace Hardware does not participate in these types of promotions, and we do not contact our customers through unsolicited text message campaigns.

Reward for Completing a Survey

These messages are similar to the previous example, except they claim they will send a gift in exchange for completing a survey. Customer survey requests that are validly from Ace Hardware are offered at the bottom of an in-store purchase receipt or sent via email to customers who make a Ship to Store or AceHardware.com order.

Order Confirmation

If you place an order on Ace Hardware.com, an order confirmation and receipt will only be sent to you electronically via email and never in a text. If you receive this type of message, you shouldn't open any links or respond and delete it immediately. The perpetrators are expecting you to be concerned and click on a link without considering its legitimacy.

If you would like to see if an order was placed using your account, sign in directly using the Ace Hardware app or go to acehardware.com

How to Report Scams/Fraud

To report it directly to Ace Hardware by submitting this form.

To report it to the Federal Trade Commission (FTC), forward the email to spam@uce.gov or visit their website ftc.gov.

To report it to the Anti-Phishing Working Group (APWG), forward the email to reportphishing@apwg.org.