Fraudulent activity precautions

Phishing emails and individuals posing as Cardinal Health employees

Over the past week, customers have notified us that individuals have presented themselves as a Cardinal Health employee by contacting customers via phone and email requesting their Cardinal Health account number. This industry-wide issue of fraudulent schemes designed to steal customer account numbers, place fraudulent orders and inappropriately access product has increased as we continue business during the COVID-19 pandemic.

The safety and security of our nation's pharmaceutical and medical product supply is a top priority for Cardinal Health and a responsibility we take very seriously. A safe and reliable drug and product supply is central to our customers' business and critical to the health and well-being of patients.

Maintaining a secure supply chain takes all of us. To help you better identify fraudulent activity, please see below for some **precautions you can take**.

- If you get a call from someone you don't know who identifies as a Cardinal Health employee, you can take down their name and phone number and reach out to your sales representative or your account manager to confirm the person is a Cardinal Health employee.

- **Remember**, products that **your** pharmacy has been invoiced for should always include a Return Authorization (RA) form attached to the tote prior to being picked up by your courier driver. **Always ask to see your courier's work ID prior to handing over any product.**

- **Never give out your Cardinal Health account** number to any individual who contacts you and requests that information.

- **Review the information security tips on general phishing, wire fraud, information vigilance and passwords on page 2.**

If you encounter any of these scenarios, or are asked for your Cardinal Health account number, please notify the Cardinal Health Security Operations and Intelligence Center (SOIC) at 888.880.7642 of the incident.

Thank you for your support and your commitment to a safe and secure supply chain.

Information Security

Cardinal Health takes protecting your data seriously. We have a mature security awareness program directed at employees to make sure they think before they click. Scammers have gotten away from the foreign prince scams but are now targeting business processes.

General Phishing

Hackers use short emails with minimal details to encourage individuals to take action. Be wary of emails from unknown senders, no context emails (emails with just invoice or delivery, no order descriptions), or pressure to click links and provide data. **See the example of fraud email on page 3.**

Wire Fraud

A common scam hacker attempt often includes impersonating managers, customers, or vendors and requesting funds or changes to existing payment details. Hackers spend a significant amount of time making these communications look professional.

For any change request always:

- Validate any payment instructions received by email, even from contacts you work with consistently.
- Call the contact that you have used previously. Do not trust contact details in unexpected emails. Speak directly to the person requesting the change, using contact information you know to be correct.
- Carefully review the request to ensure the email address and all the contact information is the same as emails you have received previously.
- Review the language and grammar used in the email. Make sure the tone is similar to previous correspondence.
- Validate current information. Ensure the request has details regarding the current account.
- Still unsure? Call your sales representative or the Cardinal Health support line directly.
- Carefully review all payments before you send them. Ensure all correspondence is validated and internal controls are followed.

Information Vigilance

LinkedIn, Facebook, public websites and press releases have a multitude of organizational details. Hackers will often use tidbits they find online to trick individuals into believing their scam. Be careful about the information you share online and understand that criminals will use organizational details to complete their story.

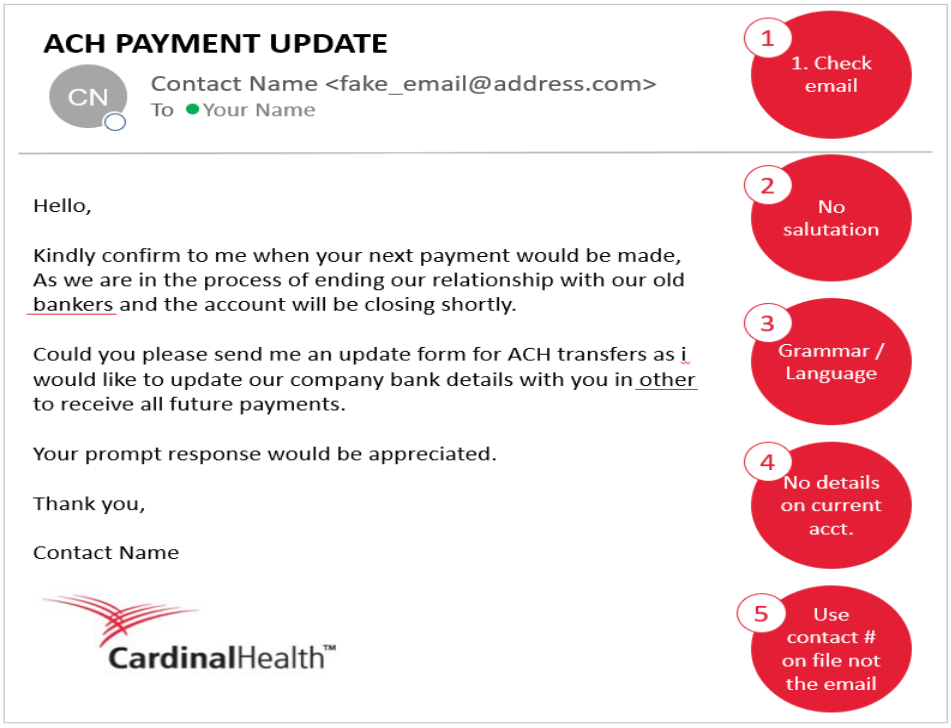
Passwords

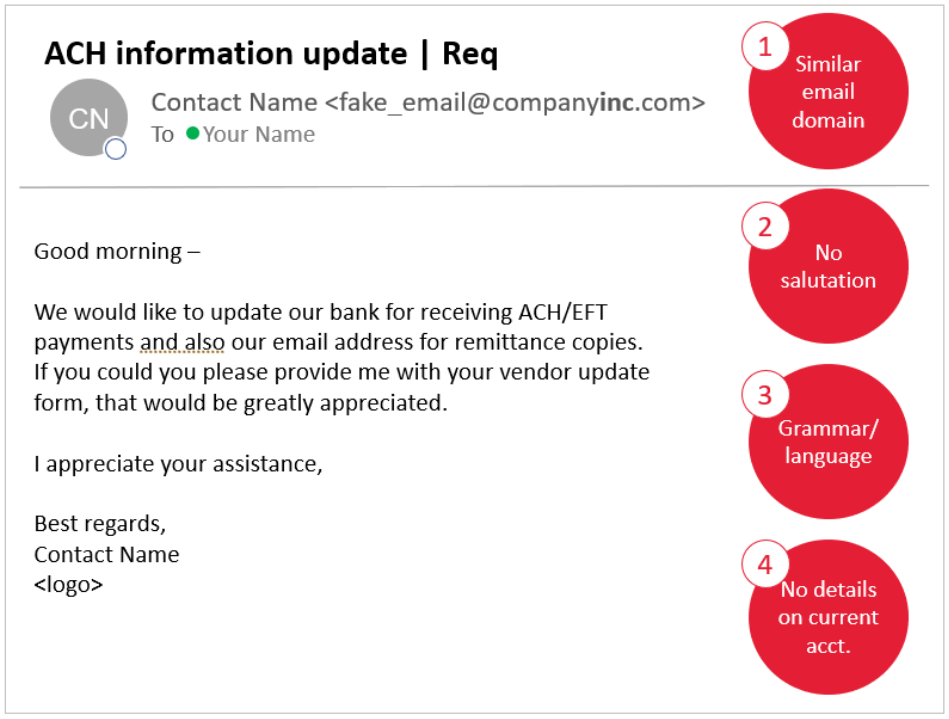
If you access Cardinal Health accounts, it is imperative you have a unique password for that account. Hackers often ‘stuff’ passwords with known emails and password combos in hopes of gaining account access.

- Never share your Cardinal Health password.
- Make sure the password is unique and long.
- If available, utilize multi-factor authentication

If you are sent an email to access your Cardinal Health account, or other sites with confidential data, always hover over the link to see what the web address is. If you are presented with a screen to enter in login information, always double-check the web address at the top is the correct web address.

Examples of a fraud email





What can you do?

- Be 'Cyber-mindful' – Think before you click
- Follow your internal process
- Call the number on file for your contact. Speak directly to them
- Have requestor validate current bank information on file
- Contact your sales representative or account manager