Capital Pump & Equipment

Cyber Security Newstetter

June 2024

What is "phishing"?

Phishing emails look like they came from a person or organization you trust, but in reality, they're sent by hackers to get you to click on or open something that will give the hackers access to your computer. This can lead to serious consequences, including unauthorized access to our valuable data and potential harm to our operations.

Why are you at risk?

Hackers are actively targeting Capital Pump and Equipment because we have valuable information. Specifically, they may be interested such as customer, employee data, intellectual property, financial account information, or payment card data. Capital Pump and Equipment's entire system can be accessed if one employee falls for a phishing attack.

How to spot a phishing email

Hackers have cleverly designed their emails to make them look legitimate. But phishing emails often have the following characteristics:

- Ask you for your username and password by replying to the email or clicking on a link that takes you to a site where you're asked to input the information.

IMPORTANT: Nobody at Capital Pump and Equipment will ever ask you for your password.

- It looks like they come from the HR or IT department.
- The email has grammatical errors.
- Contain email addresses that don't match between the header and the body, are misspelled (like *@gmaill.com*), or have unusual formats (*@company-othersite.com*)
- Have links or email addresses that show a different destination if you hover over them.
- Try to create a sense of urgency about responding.

What you should do if you get a suspicious email

- Do not open any links or attachments in the email
- Notify IT Point of Contact at **@480.340.4272**
- If you've already opened a link or attachment, disconnect your computer from the Internet but do not turn it off, and **immediately call IT @480.340.4272**
- Please be advised that Capital Pump & Equipment will NEVER ask you to change or provide payment information, passwords, or other sensitive data via email.
- Our policy is to only discuss payment updates over the phone from a verified company number or in person.
- If you receive any suspicious emails claiming to be from us and asking for payment info:
- Verify the Sender: Check the sender's email address carefully. Sometimes, scammers use similar-looking addresses to impersonate legitimate companies. Look for any misspellings or unusual domain names.
- Call CPE directly at our published company number (480-626-5257) : If in doubt do not send payment until you verify the invoice, company and client through phone call or trusted email.
- Mark it as Spam: Most email services have a built-in spam folder. This helps train the filter to recognize similar messages in the future.
- Do not Click on Links or Download Attachments: Avoid clicking on links or downloading attachments from unknown or suspicious emails. These could lead to phishing sites or malware.
- Report it: if you are receiving phishing emails pretending to be from Capital Pump & Equipment, please notify our accounts receivable team ar@cpepumps.com immediately.

- Protecting your personal and financial information is of utmost importance to us. Please remain vigilant against these phishing attempts.
- Capital Pump and Equipment stands committed to safeguarding and protecting your information and providing training and awareness as needed.

If in doubt reach out