

Title: Don't Take the Bait – 6 Timely Tips to Help Avoid Phishing eMails.

Author: Dennis O'Connell, Director of Security Solutions, Custom Computer Specialists

Phishing emails are a common way for cybercriminals to steal important data from healthcare facilities. This article will discuss what phishing is, how to identify a phishing email, and how to protect your facility's data from being stolen. We will also provide tips for avoiding phishing scams, the consequences of falling for a phishing scam, and how to report a phishing email.

This article covers:

1. What is phishing, and how does it work
2. How to identify a phishing email
3. How to protect your business data from being stolen
4. Tips for avoiding phishing scams
5. The consequences of falling for a phishing scam
6. How to report a phishing email

Facilities of all sizes are at risk of a data breach, and the consequences can be devastating. Hackers can steal sensitive information such as passwords or credit card numbers, and they may even be able to access confidential patient information, damage a facility's reputation in the process.

## **1. What is phishing, and how does it work**

Phishing is a type of online fraud involving emails or websites that mimic legitimate businesses to trick individuals into providing sensitive information, such as passwords or credit card numbers. Cybercriminals will often create emails or websites that look very similar to those of a legitimate company, and they may even use the company's logo or branding. When an individual clicks on a link in a phishing email or visits a phishing website, they may be taken to a fake login page where they are prompted to enter their username and password. Once the cybercriminal has this information, they can use it to access the individual's accounts or steal their money.

## **2. How to identify a phishing email**

You can look for several things to determine if an email is a phishing scam. First, check the sender's address to see if it matches the company's address that it claims to be from. If the sender's address is different or if there are typos in the address, it is likely a phishing email. Second, look for generic greetings such as "Dear valued customer" instead of your name. Third, be suspicious of any email that asks you to click on a link or download an attachment, as these could contain malware that will infect your computer. Finally, trust your gut – if something about the email feels "off," it is probably a phishing email.

## **3. How to protect your facility's data from being stolen**

You can take several steps to protect your data from being stolen in a phishing attack. First, educate your employees about phishing scams and make sure they know how to identify a phishing email. Second, use a spam filter to block emails from known or suspected phishing websites. Third, do not click on email links unless you are absolutely sure they are legitimate. Fourth, do not download attachments from unknown senders. Finally, keep your anti-virus software up to date and run regular scans on your computer to ensure it is free of malware.

#### **4. Tips for avoiding phishing scams**

You can do several things to avoid falling for a phishing scam. First, be suspicious of any email or website that asks you for personal information. Second, do not click on email links unless you are absolutely sure they are legitimate. Third, do not download attachments from unknown senders. Fourth, keep your anti-virus software up to date and run regular scans on your computer to ensure it is free of malware. Finally, if you are ever unsure about an email or website, you can contact the company directly to confirm its legitimacy.

#### **5. The consequences of falling for a phishing scam**

If you fall for a phishing scam, the consequences can be severe. Your personal information may be stolen and used to commit identity theft, and your computer may be infected with malware. You may also lose money if you provide your financial information to a phishing website. In addition, falling for a phishing scam can damage your reputation and cause you to lose trust in online communications.

#### **6. How to report a phishing email**

If you receive a phishing email, do not reply to it or click on any links. Instead, report it to the company from which it claims to be and to the Federal Trade Commission (FTC). You can also forward the email to the Anti-Phishing Working Group at [reportphishing@apwg.org](mailto:reportphishing@apwg.org).

Don't hesitate to reach out to your MSP or Custom Computer Specialists and we'll assist you with any questions you may have about security or identifying phishing emails. Also, be sure to ask us about security awareness training to strengthen your first line of defense, your employees. I can be reached by phone at 631-761-1463 or email at [doconnell@customonline.com](mailto:doconnell@customonline.com)