Bryan Jick

From: athenahealth Customer Success <CustomerSuccess@comms.athenahealth.com>
Sent: Friday, June 11, 2021 6:01 AM
To: Bryan Jick
Subject: QuickPay Portal scam sites – how to protect patients

athenahealth

Are your patients paying on the right site?

In the past several months we've seen fraudulent websites emerge online that attempt to solicit payment from healthcare patients. Some of these websites seek to mimic athenahealth's QuickPay Portal.

Our QuickPay Portal is secure. However, fraudulent look-alike websites with similar names have begun to appear in internet search results. While patients should only make online payments using the URL provided on their patient billing statements, we've heard reports of patients being tricked by internet search results.

We're making significant investments to combat this problem on behalf of our customers and their patients.

Here is what we're doing to fight back against these bad actors:

1. Our teams are regularly searching for and taking action on imposter websites. We're directly engaging with domain registrars and web hosting companies to take these sites offline.
2. We're changing our patient billing statements to reduce the potential for error and risk of online fraud. These changes include:
    - Adding an insert into patient bills with clear guidance on how to safely access our QuickPay Portal
    - Adding a QR code onto all patient bills, which we'll encourage patients to use, so that there's no risk of them mistyping the URL of our online payment portal
3. We're working with Google and other online search engines to ensure searches for our online payment portal highlight our website

first. As part of this effort, we're improving our own website's metadata.

4. We're in the process of transitioning all of our online pay options to an athenahealth.com domain. This change will help domain registrars and search engines to more rapidly remove imposter websites.

We encourage you to educate your patients about the risks of fraudulent online payment websites. Here are some warning signs that they've reached an imposter site:

- The site asks for personal information (e.g. name or address) or payment balance
- Being told to call a customer service line to process a payment
- Receiving an error message such as "payment on hold," "transaction pending," "error processing your payment," "oops," etc.
- Poorly translated text and instructions for using the site
- Links to other non-athenahealth sites
- Ads – some sites don't collect visitor information but receive ad revenue for every visit. The athenahealth QuickPay Portal doesn't have any advertisements

You can leverage either or both of the tools in athenaNet listed below to contact your patients about this topic:

- create and deploy an athenaCommunicator GroupCall Custom campaign with instructions for finding and using the QuickPay Portal
- add custom text to your patient statements using Statement Notes

It's incredibly frustrating that scammers create these sites to exploit people trying to pay medical bills. We're dedicated to doing what we can to confound their efforts. If you have questions about fraudulent QuickPay Portal sites, please open a case by navigating in athenaNet to Support > Create Case or Call > Patient Billing & Payments so we can support you. If a patient believes they made a payment on a fraudulent site, they should immediately call their bank or card issuer to cancel the payment and take steps to secure their account.