

Warning: Phishing Scams Potentially Affecting Urgent Care

"Phishing" occurs when a criminal--masquerading as a trustworthy source--attempts to gain sensitive information in order to defraud. Although most of us are aware of "phishing" schemes involving credit card or online banking information, a variation of this fraud is starting to be seen in urgent care centers. Organized and individual criminal entities attempt to get personal information about a provider--including provider identifier, medical license, DEA and tax identification numbers--in order to create and submit fraudulent claims to Medicare, Medicaid, and private payers.

The scam starts with the criminal entity sending a letter, fax, or email on the letterhead of a "legitimate" payer requesting confirmation or updates of sensitive information about a provider. Such correspondence may be sent to a provider's office or home. Usually there is a deadline--such as 48 hours--to respond to avoid "interrupting payment." An unsuspecting provider or office assistant may return the information, giving the criminal entity all the information it needs to contract with and/or submit bills to a payer using the provider's identity. The payer--believing the claims are legitimate from a "known" provider--pays the claims as required by prompt pay statutes. A proficient criminal entity can collect up to \$100,000 per day in claims--directly deposited to its bank account--before the payer's systems flag the provider for possible fraud. When investigated, the provider rarely realizes he or she has been implicated in a criminal scheme.

A similar variation occurs when the criminal entity sets up an "employment" website, requesting provider information as part of a job application, reference or background search.

As with personal identity theft, medical provider information theft causes hassle in lost time, leads to delay in reconciling payment, incur unnecessary legal costs, and permanently damage a provider or practice's reputation. The best way to safeguard against "phishing" schemes is to raise awareness among staff members that all business, provider, and patient information should be guarded and only released to authorized entities that have been identified. A legitimate payer will not request sensitive information using unsolicited correspondence--if there is ever doubt about the legitimacy of a request, contact the payer directly using a known and published number (not the number on the questionable correspondence).

Submitted by Alan Ayers