Protecting Our Patients

Cybersecurity at Wellstar

Wellstar and all health systems across the U.S., have received a special advisory regarding healthcare-targeted ransomware attacks. Over the past few months, a number of hospitals have been impacted by ransomware, designed to block access to a computer system until a sum of money is paid. These attacks use different methods like spam and phishing campaigns to try to breach important technology systems such as electronic medical records, in an effort to make it very difficult to ensure patient safety.

Please pay very close attention to all your email and do not click on attachments that look suspicious. As we approach the holiday season, cybercriminals bombard unsuspecting email users with spam and phishing attempts to breach important technology systems such as electronic medical records. Please pay close attention to all your emails and DO NOT click on links unless you are 100% certain it is safe. Consider calling the sender to confirm they sent you a link or attachment, hover over links included in emails to confirm where it will take you and verify the sender's email address.

Review the reminders below and reinforce the importance of cybersecurity with your team members.

Suspicious email examples include:

- Shipping Notifications asking you to verify your information or track a package
- Email Promotions from companies with which you do not normally do business
- Holiday eCards and Party Invites asking you to download a link or attachment
- Email Links and URLs to entice you to copy/paste links or click on malicious documents and/or links

If suspicious, follow these in the Outlook email toolbar:

- Locate the Report Message button
- Select Phishing
- Click Report

Call (470) 956–6000 if you have any concerns or questions related to cybersecurity.

Wellstar HEALTH SYSTEM