SECURITY INSIGHTS:

Encoded URLs are Used to Bypass Secure Email

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

In today's digital world, we're all familiar with the importance of being cautious about clicking on suspicious links in our emails. However, cybercriminals are constantly finding new ways to outsmart our defenses, and their latest tactic is both clever and concerning. Cybercriminals have discovered a sneaky method to bypass our email security systems. They're now using something called "encoded URLs" to hide malicious links in emails. This technique makes it harder for security software to detect these harmful links, increasing the chances that unsuspecting users might click on them.

Many companies use Secure Email Gateway (SEG) as a layer of email protection. A secure email gateway essentially rewrites every URL in an outgoing email into a link pointing to its infrastructure. When a recipient clicks on the encoded link, the user is first directed to the SEG system, which checks if the URL is safe before redirecting the user to the intended destination. The checks usually involve assessing the URL using reputation, blacklists, signatures, and other mechanisms, which means sometimes it might take an SEG days and even weeks before it designates a URL as malicious.

Encoded URLs work by converting special characters, unsafe characters, and non-ASCII characters into a format that can be safely transmitted and processed by web servers and browsers. Special characters are converted to a percent sign (%) followed by two hexadecimal digits representing the character's ASCII code. For example, common encodings include "spaces" becoming %20 and reserved characters like "?" and "#" being encoded as %3F and %23, respectively. This encoding allows URLs to contain characters that would otherwise be invalid or have special meanings in URL syntax.

The problem is that, often, when SEGs detect URLs in emails that are already encoded, they do not scan them, passing them right through to the user.

While this new threat is concerning, there are steps you can take to protect yourself:

- **Be skeptical:** Even if an email looks like it's from a trusted source, always approach links with caution.
- **Don't rush:** Cybercriminals often create a sense of urgency. Take a moment to think before clicking.
- **Verify independently:** If an email asks you to log in to an account, go directly to the website by typing the address in your browser instead of clicking the link.
- **Educate yourself:** Stay informed about the latest cyber threats. The more you know, the better prepared you'll be to protect yourself and others. Share this knowledge with friends and family to help them stay safe online.

This new tactic is part of a broader trend of sophisticated cyber attacks. It's a reminder that our online safety requires constant vigilance and adaptation. By staying informed and following best practices, we can make it much harder for cybercriminals to succeed. Remember, your online safety is in your hands. Stay alert, think before you click, and err on the side of caution when in doubt.