Phishing attacks: Watch out for these telltale signs that you've been sent to a phoney website

Sometimes the simplest techniques can trick people into falling victim to hackers – but here's a few things to watch out for.

The number of phishing attacks continues to rise and cyber criminals are using some very simple techniques to ensure that their malicious emails bypass security protections and trick victims into downloading malware, potentially handing over their login credentials and more.

Researchers at cybersecurity company examined over 25,000 malicious emails that had bypassed inbox security over a three month period and found that rather than using advanced techniques, many of the attacks were simply redirecting users to fake websites.

Often, these sites pose as big-brand companies like Microsoft, PayPal, banks and retailers, and encourage users to enter personal credentials. If the user provides this information, it falls into the hands of the cyber criminals who can use it in any way they wish, either for committing fraud and theft themselves, or selling the credentials on to others on underground forums.

However, examination of the phishing websites found that there are usually some telltale sign that the page is a fake – even when the sites were designed to look like copies of the company they're mimicking.

In almost half of cases, **images on the website were blurred and out of focus** – a sign that the images have been screen-grabbed or otherwise copied from the real thing and placed on a fake. In a quarter of cases, the **image had been resized and appeared stretched or elongated**. In both of these cases, it's usually a sign that something is wrong.

Meanwhile in around 15% of cases, phoney sites are **designed in such a way that they look different to the real version**; in many cases, these fake landing pages pass themselves off as having had a redesign.

In about one in ten cases, the phishing page looks almost legitimate, but attackers have chosen **outdated imagery or messaging on their fake website**. This can happen if a company has changed its logo or branding and the attackers haven't paid attention to the websites they're trying to mimic.

In 5% of cases, the phishing website will look and sound a lot like the company the attackers are trying to mimic, but **displays an uncommon sense of urgency for the visitor**, be it a threat of something having gone wrong, or telling them they need to enter their details immediately to access their account.

In many cases, peoples miss these clues and fall victim to phishing websites due to intentional blindness: when you don't see an unexpected change, even when it's hidden in plain-sight.

However, if users spend a few seconds examining potentially suspicious emails and websites, clear indicators of the messages or the web page being false can often emerge.

Look for common typos, sometimes emails look legitimate but these could give away that they're not. Hover over links and see where they're actually going – does it, for example, actually go to the actual real address?

And if users really think they need to enter their credentials, it's recommended that they go directly to the website that the email claims to link to, so as to avoid the possibility of clicking a malicious think and handing their details to attackers.

If you get an email claiming to be from a website, don't follow the link but go to the actual website by typing out the main URL instead of following the link. And if you think you've done something like click on a phishing link, don't be afraid to ask for help.

The best thing to do is to make your Department IT, University Information Technology (UIT) and/or UND IT Security Officer team aware of anything suspicious or unexpected.

Contact Info:
UND IT Security Officer
CFL, Rm 131C
701-747-5860