22 March 2019, 16:31 (GMT)

‘Phishing’ Scammers Target Leading Irish Web Provider

Customer data has not been breached, says Blacknight

An Irish internet provider has warned of an increase in ‘phishing’ attacks, targeting their customers.

Typically, phishing attacks tend to impersonate banks and financial institutions, with emails telling them to click a particular link to ‘resolve a problem’. But the link leads to a fake page, masquerading as a legitimate website, which aims to trick the users into entering personal data, such as usernames, passwords, and even payment card details.

But scammers don’t need to impersonate a bank to get valuable information. Utility companies, major retailers and online services have also been the target of phishing attacks. And the latest attack is focussed on a leading Irish web hosting company.

Based in Carlow, Blacknight provides web hosting, email and cloud services to more than 90,000 customers in Ireland and abroad. Over the last few weeks they've become aware of a series of phishing attacks using their company name and branding.

"The first thing is to reassure our customers", says Blacknight's CEO Michele Neylon. "There has been no breach of customer data held by Blacknight. Our security is ISO-certified and subject to frequent audits".

"If you've received one of these emails, they didn't get your address from us. We know this because we've had reports from people who don't have an account with us. That's why it's called 'phishing'. Millions of these emails are sent out, 'fishing' for victims, and using the identities of major brands as bait".

Mr Neylon said that Blacknight has been working to combat the fake sites, working with other providers internationally and getting them taken down, usually within minutes of the first report. But the scammers have continued to set up sites on new domains and to send phishing emails. He stressed the importance of the public's assistance in reporting phishing crime, and outlined a number of clues people can use to check that an email is genuine.

- Bad grammar is usually a frequent giveaway. Legitimate companies take care to present their corporate communications in a way that reflects well. Sloppy English can be a sign of a scam.
- Look carefully at the link you are being asked to click. The linked text may look like a normal blacknight.com address, but the actual link it points to may be different. Does a different link address appear in the status bar at the bottom of the window when you put your mouse over the linked text? Don't click it.

- If you have clicked the link, look at the address bar at the top of the browser window. Look at the hostname (or domain name) part of the address. This is the part after 'https://' and before the next '/'. This should contain only blacknight.com, or www.blacknight.com, or cp.blacknight.com. It should not contain any other words. If it says something else, it is a fake.
- Blacknight sites use Digital Certificates with Extended Validation (EV). This means that the connection is secure, and also that the domain name has been independently verified as belonging to Blacknight. You should see this beside the padlock icon, the full company name with the Irish country code: "Blacknight Internet Solutions Ltd [IE]". (Mac users of the Safari web browser will see the domain name highlighted in green, and they can click on the padlock to see the company details). If you don't see this information, it's not Blacknight.

"It's a price of success, unfortunately", said Neylon.

> *"It's inevitable, when you reach a certain size of customer base, that thieves will try to use your name to con people. But we've been fighting fraud for years and advising our customers how to deal with it, and we know that a prompt and pro-active response is the most effective action. That's why we're appealing to the public to be alert, and to help us by forwarding the fraudulent emails to our abuse desk, so we can get them taken down as soon as they appear".*
>
> — Michele Neylon, CEO, Blacknight

So what should you do if you receive a suspicious email?

"Don't click the link", says Neylon. "If you do click it, don't enter any personal data. And if you are worried that you have been scammed, contact us by email, live chat or phone and we'll do our best to help".

ENDS

Further comment or interview:

Michele Neylon
CEO
+353599183072
michele@blacknight.com
mneylon

Photo: Michele Neylon, CEO, Blacknight

ABOUT BLACKNIGHT

Blacknight (http://www.blacknight.com/) are an Irish based, ICANN accredited domain registrar and hosting company. Recipients of several awards for their revolutionary use of social media, Blacknight are one of Europe's most cutting edge Internet companies. Blacknight constantly seek to lead the way by introducing innovative solutions for its client base and provide dedicated servers and co-location as well as a comprehensive range of Microsoft Windows and Linux based hosting plans and domain name registration services to business globally. IP transit services and other solutions for more demanding business and academic customers are offered a la carte.

Blacknight