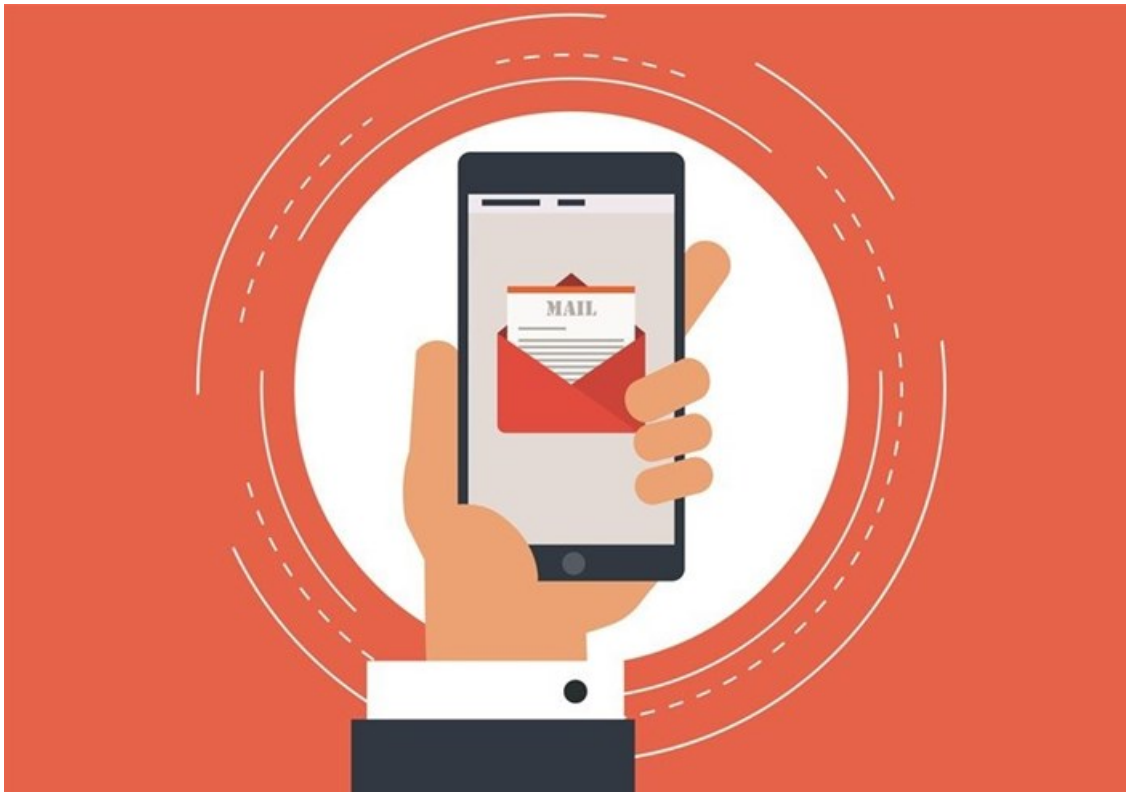
BIZCOMMUNITY

It's high time for dealing with spam and phishing

It's the silly season, and while most go shopping, cybercriminals go phishing. With the larger volumes of promotional emails hitting inboxes over the festive and back-to-school period, now is the time for companies to step up email management.

“Companies can help protect their users and businesses from becoming phishing victims by putting a good email phishing and Business Email Compromise strategy in place. Especially over the festive season, there is a dramatic rise in spam, promotional emails and phishing emails.



“For organisations who have a holiday break coming up over December, it is a good time to get a Phishing and Business Email Compromise (BEC) strategy in place, test the technology properly and get everything up-and-running while there are fewer people in the office, before the New Year starts,” says Charl Ueckermann, CEO at AVeS Cyber Security.

He explains that phishing is the fraudulent process of getting information like passwords, usernames, credit card numbers, banking details, business information and other sensitive information by posing as a company or person that the receiver recognises or trusts.

> Phishing emails are always made to look like the real thing from banks, popular social networking websites, retailers, internet service providers and sometimes even as a company’s email administrator. As phishing emails are so well disguised, conventional email security solutions can fail to detect them.

“The emails often contain a link to draw the recipient to a fake website where they erroneously give away sensitive or personal information. Cybercriminals use this information to steal money, steal identities, steal business information and conduct all manner of fraudulent activities. It can impact users individually or the business as a whole,” says Ueckermann.

Companies can consider installing technology that is capable of blocking certain components of emails, corrupted emails and even label emails in the subject line. Ueckermann notes that there are a few technology solutions that offer next-generation email protection.

The solutions detect and stop spam and malicious email before it becomes a problem and without slowing down productivity. Companies can also rest assured that legitimate emails won't be deleted by mistake. Leading Email Security software includes features such as advanced heuristics, sandboxing and machine learning to protect email from spam, phishing, Business Email Compromise (BEC) and other advanced threats. It gives companies complete control over what happens to suspicious emails and includes the latest spam, phishing, malware (including ransomware) protection and advanced attachment filtering.

Forcepoint reveals cybersecurity predictions for 2019

23 Nov 2018

Ueckermann says there are some important things to consider when implementing a strategy and technologies to address phishing and Business Email Compromise (BEC).

"In today's digital-driven business environment, a great user experience is vital for improving productivity, employee morale and technology adoption in the organisation. Don't stop people from receiving business emails; rather put mechanisms into place to ensure that only legitimate emails arrive in their inboxes. These mechanisms must not hamper productivity in any way or stop legitimate emails from getting through. The technology should detect and stop dubious emails; it should ideally not be left up to users or administrators. As we know, phishing emails are well disguised, and it is difficult for a non-technical person to know what is legit and what is not.

> *"As a business owner or IT Executive, look at a number of emails people are getting and compare it to the industry norm to determine what you can cut out. Also, look at the type of content employees receive and cut out what might be of danger to the organisation. The same Email Security software described above can give you statistics on how many emails coming into your organisation have malware in attachments, spam or are potential phishing attacks. This will also help you understand how big the problem is within your organisation compared to industry norms. If your email risks are high, you can use these statistics to plan appropriate user awareness among business email users."Cost and the manageability of these solutions are obviously key considerations. Companies should aim to deploy the most effective and easiest to manage solutions that they can afford. Free or open source solutions will not offer the level of protection needed to stop the latest threats, as they're often the source of these security backdoors."*

If people are more aware, they will tend to protect the company on their own.

He points out that deploying technology is only half of the solution. User education is the other half.

"When a phishing email manages to get in, it is pretty harmless until the recipient opens it, clicks on links and ventures onto an unsafe website to disclose information they should not be disclosing. That is why it is important to educate employees about the dangers of phishing and how they put themselves – and the business – at risk."

Ueckermann offers these tips for employers to guide employees on keeping their business email inboxes clean:

- Don’t use company emails for social media profiles
- Don’t buy stuff online using company emails
- Don’t wait for someone to teach you safe email practices, self-educate and ask experts in the organisation; there are many free resources made available by industry experts via social media, such as how-to videos and quick-tips articles.
- Understand the dangers of opening or clicking on links in emails
- Treat unsolicited emails requesting sensitive information with suspicion
- When subscribing to websites, use other email accounts, such as a separate Gmail account
- Don’t sign-up for newsletters using their business email addresses.

Ueckermann concludes by saying that companies can enforce their rights to protect networks and data with formal policies on social media usage, password changes, IT security, browsing the internet and email usage.

“These policies formalise an organisation’s standpoint on the usage of their internet and email resources without complicating it. Accompanying technologies to address each problem will help to enforce the policies. Employees should be made aware of these policies as well as the consequences of non-compliance.”