


Phishing Emails Have Become Very Stealthy. Here Are 5 Ways to Spot Them Every Time

 inc.com/neill-feather/phishing-emails-have-become-very-stealthy-here-are-5-ways-to-spot-them-every-time.html

July 17,
2019

Phishing scams are nothing new. In fact, we've all heard about the "Nigerian prince" phishing emails that have been showing up in inboxes for years.

Unfortunately, phishing attacks continue to increase exponentially in volume, and are considered a serious threat to both companies and individual internet users since they can result in devastating financial losses. In addition, phishing emails can be much harder to recognize than many business owners think.

Cybercriminals have resorted to increasingly sophisticated phishing strategies as of late to get recipients to open, click, and share malicious code. And these tactics are paying off handsomely. Business email compromise (BEC) scams are more successful than ever, with losses reaching \$2.7 billion in 2018.

Here are some common phishing trends that business owners should know about and tips for educating employees about them:

What are phishing scams?

Phishing scams typically consist of emails that seem harmless but are actually intended to trick users into sharing sensitive information. This is often accomplished by encouraging the user to click on a malicious link or attachment. Phishing emails get their name because the hackers are "fishing" for your personal information.

Most phishing emails appear completely legitimate, often by imitating a company's logo using high-quality graphics and including opt-out instructions. For this reason, it's quite common for recipients to be fooled, and even large companies have fallen prey to these scams. SiteLock has published a round-up of some recent phishing examples to demonstrate the prevalence of these scams and how to protect against them.

Common Phishing Trends and Techniques

There are many different techniques hackers use to launch a phishing attack. A few of the most common ones are provided below:

- **Invoice phishing:** Invoice phishing scams emails claim the recipient has an

outstanding invoice from a well-known company, bank, or vendor. The email instructs the recipient to click on a link to pay their invoice. But when they click on the link and access the site, the hackers steal their personal information and gain access to their bank accounts.

- **The virus or compromised account:** Viruses and compromised accounts cause users to receive an email from a third party company claiming one of their accounts has been compromised. The email instructs them to log in to reset their password or to download a form, fill in their personal information, and return it. However, a legitimate company would never request your personal information through email in this manner.
- **Payment and delivery scam:** This tactic involves sending emails from what appears to be a legitimate vendor asking for a user's credit card information. They typically claim that your payment information needs to be updated before they will deliver your order. Be very careful with these emails, especially if you haven't purchased anything from the vendor.
- **Downloads:** Download scams send an email instructing recipients to click on a link. These emails often contain hyperlinks that could download a malicious file onto the end user's computer. Never click on an email link unless you are absolutely sure that the sender is who they claim to be.

Tips for Spotting Phishing Emails

Although phishing emails often mimic actual companies and vendors, there are ways to detect them. All small business owners and employees should be aware of the following red flags that indicate a possible phishing email:

1. The email contains links or URLs that direct you to the wrong website or try to get you to access a third-party site that is separate from the email sender.
2. You receive an email from a company requesting sensitive information which can include your social security number, bank account information, or credit card numbers. Consider these emails suspect and never share your personal information without checking with the company first.
3. You find an unexpected email in your inbox from a person, vendor, or company that you rarely or never deal with. If this happens, the safest thing to do is delete the email without opening it, as there's a good chance it's a phishing email.
4. The email has obvious errors like typos, poor grammar, or incorrect information. A legitimate email from a company is very unlikely to have these kinds of errors.
5. The email address of the sender is incorrect, although it is close to the actual email address. This is another common sign of a phishing email.

Phishing scams remain a very common type of cybercrime, and can cause major financial losses to individual users and companies. And phishing emails are much more sophisticated these days, making them harder to detect. If you're a business owner, it's essential to be aware of common phishing techniques and red flags and to educate your employees on them. By doing so, you can help protect your company from financial losses and other serious consequences of phishing.

Published on: Jul 17, 2019

The opinions expressed here by Inc.com columnists are their own, not those of Inc.com.