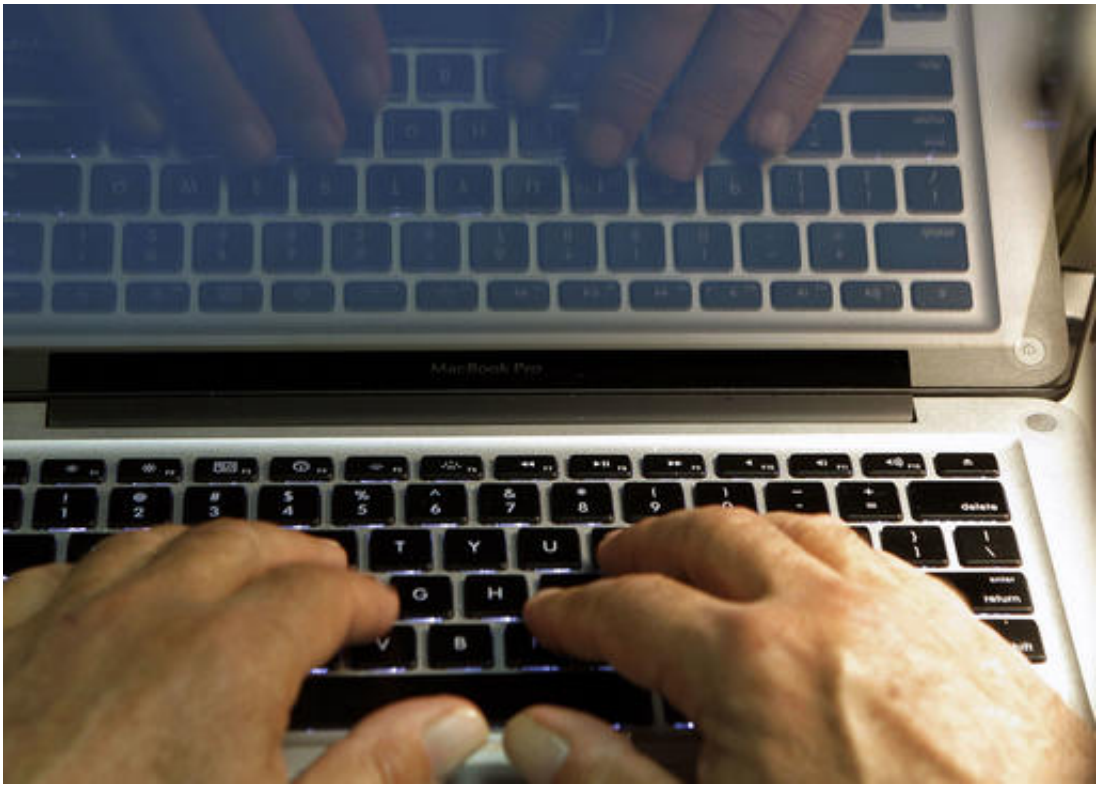
Phishing season in full swing as tax deadline looms

March 9 2016, by Bree Fowler



In this Feb. 27, 2013, file photo illustration, hands type on a computer keyboard in Los Angeles. As tax day nears, phishing season is in full swing. The IRS says it's seen a "surge" in phishing emails in 2016. And thieves are also baiting special hooks for payroll and human resources workers, in hopes of snagging a company's entire stash of employee information. (AP Photo/Damian Dovarganes, File)

Tax day is a little more than a month away, which means phishing season

is in full swing.

The IRS says it's seen a "surge" this year in phishing emails, with thieves baiting special hooks for payroll and human-resources workers in hopes of snagging a company's entire stash of employee Social Security numbers and other personal information.

Meanwhile, tax-season phishing attacks against individuals are also up. Last month, the IRS said it had seen a quadrupling of phishing- and malware-related incidents for this year's tax season.

Experts warn that phishing emails often masquerade as legitimate communication from your bank, human resources department or email provider. But in reality, they're part of a scheme designed to steal the confidential information stored in your computer, or to gain access to the network it's attached to. And this time of year, that information can be used to file a false tax return.

While people are more aware of the danger of phishing more than ever before, the lures continue to evolve and increase in sophistication, making it tough for the average person to discern which emails are legitimate and which ones aren't.

Here are a few answers to common questions about phishing:

___

WHY IS IT SO BAD THIS TIME OF YEAR?

Phishing peaks during tax season, partially because it's a time of year that many people are accustomed to entering their most personal information—such as their Social Security number or bank account information—on websites, Satnam Narang, senior security-response

manager for security software maker Symantec, says.

Thieves can then use that captured information to file a false return.

Phishing also spikes around Christmas, with attacks in the form of fake delivery notifications. Thieves also often tie phishing emails to major sporting events, or natural disasters like overseas earthquakes, says Raj Samani, chief technology officer for Europe, the Middle East and Africa at Intel Security.

"They're very much up with the latest news and information," Samani says. "If they can spend a little more time and get a 0.1 percent increase in click-throughs, then their campaign becomes hugely more profitable and successful."

___

WHAT'S THE DIFERENCE BETWEEN PHISHING AND SPEAR FISHING?

Narang likens phishing to a person casually throwing a rod in a lake and waiting for a bite. Phishing emails don't contain a lot of specifics, but are quick and easy to send out in mass quantities.

"Spear phishing" is much more targeted and personalized. The people behind those attacks spend time researching their targets in order to create highly customized emails that look much more legitimate and are much more likely to be clicked on.

The rise of social media has made this a lot easier. Thanks to Facebook and Twitter, details including a person's place of employment, where they bank, like to shop and the names and ages of their children are just a few clicks away.

___

WHAT OTHER RED FLAGS SHOULD I BE ON THE LOOKOUT FOR?

In an effort to get more people to click on a link before thinking about the possible consequences, many phishing emails will give an impression of scarcity, or include some kind of time limit.

For example, an email made to appear to be from a person's bank or email provider may state that if that person doesn't click on the enclosed link within 24 hours, they will be locked out of their account.

And while poor English and long, complex web links were previously sure signs of phishing, they're not as prevalent anymore. Many overseas hackers are no longer using clunky translation websites, because there are fluent English speakers who specialize in translating phishing emails for a fee, Samani says.

Meanwhile, it's become easier to shorten the Web links that direct a people to fake websites, he says.

Narang adds that people should be wary of emails purported to be from banks, or other companies they do business with, but didn't opt into emails from. He also notes that banks generally don't include Web links in emails.

Those links will likely take a person to a fake website where they will be asked to login and those credentials will ultimately be stolen, he says.

And attacks don't just come in the form of email. They can come as text messages too, with those links often containing viruses, Samani says.

IS THERE ANY WAY TO PREVENT IT?

Basic cyberhygiene can go a long way toward preventing a data breach, even if a link in a phishing email gets accidentally clicked on.

Using different passwords for different accounts, two-factor authentication and changing passwords frequently all can be a big help. In addition, companies should test their employees by periodically sending out fake phishing emails to see who falls for them, Narang says.

And companies need to make sure their security keys are up to date, along with their anti-spam filters, so past bad senders don't keep getting through, Samani says.

"I think common sense goes a considerable long way," Samani says.

He adds that with any email communications, it's always better to just go straight to the main website of the entity it purports to be from, just to be on the safe side.

"I can't remember the last time I clicked on a link in an email," Samani says. "I just don't do it."