Annual tax phishing season: still no one has learnt

With tax filing season upon us, the annual tax-related cyber fraud feeding frenzy has begun, warns Fortinet.

“The Receiver of Revenue, financial institutions and security firms have been issuing the same warnings every tax season for years. Amazingly, nothing has changed and people are still being defrauded during tax filing season,” says Jonas Thulin, Security Consultant at Fortinet.

“It’s the same story every year – with tax season come fraud and phishing scams. The problem is not going away. On the contrary, we see more and more of it taking place,” says Thulin.

Thulin references a long list of recent warnings posted on the SA Revenue Service’s e-filing site. In a section dedicated to fraud and cyber-crime, SARS warns of numerous phishing mails and attempts to defraud taxpayers. These range from emails falsely advising of a refund, to mails purporting to come from banks, asking recipients to confirm their bank details for tax purposes.

“Because so many more people are online now, and accessing the internet from a range of unsecured mobile devices, the attack surface is much larger than it was a few years ago,” says Thulin. “SARS and South African financial institutions have tightened their own security and all of them use strong authentication tools, yet every year we see many people caught by phishing scams.”

Thulin notes that the simplest scam requires people to click through to a link mailed to them, where they are asked to fill in their user names, passwords or other personal details. The losses suffered can be twofold – scammers could empty out their victims’ bank accounts in a once-off raid, or they could steal their identity and go on to take out loans and transact in the victim’s name, resulting in longer-term and bigger financial losses.

Phishing attacks against companies are also growing, he says. While most companies try to exercise care in mitigating fraud losses, tax filing season is a busy time and apparently legitimate emails from SARS could result in serious losses. “A company might receive a fraudulent mail advising that a tax payment is overdue, with the details of the account to where the funds should be paid. The busy accounts department sends the account through for processing without realising that the account details are not those of the intended recipient, for example.”

Fraud can also be carried out using simple SMSes, warns Thulin. “Financial institutions often use a range of numbers for contacting customers, so it is difficult for customers to be sure if an SMS comes from their bank. You might receive an SMS claiming to be from your bank’s fraud department, asking you to call a particular number to verify a purchase made on your credit card. When you call the number, you’ll happily hand over your personal details without realising you are in fact handing this information to fraudsters.”

Thulin says end-user education and constant vigilance, in tandem with next generation security measures, are the only way to avoid falling victim to this kind of fraud. “With little recourse available, end users need to stay alert and be aware that they should never click through to a link sent to them by SARS or their bank.” Thulin says he goes so far as to use

separate browsers for transacting and web browsing, in a bid to add an additional layer of security to his online transactions. “A lot of malicious work is possible on the actual browser, so many attacks happen right on the browser. It is much harder to get an executable onto laptop to install keystroke logger in background, but of course, it is not impossible,” he says.