BIZCOMMUNITY

Criminals are targeting SMEs to file fraudulent tax returns

By Carey van Vlaanderen

22 Jul 2015

It is a well-known fact that attackers like to find low hanging fruit in order to get into an organisation's juiciest targets.

Sometimes this is through outside vendors, other times this is through phishing of individuals in an organisation of whom they can make use as a foothold to get into accounts with access to more valuable data. In this recent uptick in tax identity fraud, criminals have been targeting the HR departments of various companies in order to file fraudulent tax returns.

Many smaller companies feel that they are less apt to be targets of cybercrime because they think they have 'less value' as a target. Furthermore, they may feel they do not have the budget to protect themselves. Criminals can and will use any tidbit of information they can gather in order to increase their payout.

Five ways

In light of this, small businesses need to be every bit as cognisant of protection as larger organisations and to avail themselves of the many ways in which they can protect themselves at little or no extra cost.

1. **Two-factor authentication**: Whenever this option is available, whether for payroll companies or when using any other online services, you should enable it.

2. **Anti-phishing scanning**: When criminals become aware of poorly defended third-party sites that are of value to them, they can use their login credentials. Using anti-phishing scanners in browsers and email can greatly decrease the likelihood of users being tricked into disclosing their login credentials. While education is very helpful (and highly recommended) to prevent phishing, fraudsters can sometimes craft links that are compelling enough to trick all but the most expert users. Anti-phishing scanning can be extra helpful with those particularly deceptive phish.

3. **Anti-malware technique and technology**: Criminals may also target users with malware that has keystroke logging, which would allow them to steal login credentials without having to trick users into going to a phishing site. The usual anti-malware advice applies here: be sure to keep all your software up to date, educate your users about when it is unsafe to open attachments, and use updated anti-malware and firewall software.

4. **Network segmentation**: The best way to limit the damage should a criminal gain access to an organisation is to set permissions within your organisation. Allowing access to only those things a user must access, in order to do his or her job.

5. **Encryption**: Encrypted data may be less accessible and thus less valuable to criminals. When data has been transferred onto disks, make sure that they are encrypted. Most major operating systems offer this ability at no extra cost. Encrypting sensitive data in transit is important too. Email and IM are not generally encrypted, unless you use a separate program designed to encrypt this traffic. Web traffic may be encrypted - look for HTTPS or a lock icon at the beginning of a URL to see whether the traffic has been secured. (But be aware that phishing sites sometimes use fake lock icons to inspire misplaced confidence in the unwary user.)

Whether your business is big or small, the methods are much the same (small businesses simply have less organisational and technological complexity). Thankfully, as protection technology has improved, it has also become cheaper and easier to access and to use effectively. By taking the time to apply these protections, businesses can make themselves less attractive to criminals.

ABOUT CAREY VAN VLAANDEREN

Carey van Vlaanderen is CEO of ESET Southern Africa. ESET is a global provider of security software for enterprises and consumers and is dedicated to delivering instant, comprehensive protection against evolving computer security threats.
- Criminals are targeting SMEs to file fraudulent tax returns - 22 Jul 2015

View my profile and articles...

For more, visit: https://www.bizcommunity.com