CYBER SECURITY WATCH NEWSLETTER

4-03-16 Volume 1

Ros Prince a partner at Shlegal writing on fraud prevention says in summary that "Sophisticated email scams/fraudsare usually addressed to individuals within the business who have the power to direct payments. The sender may appear to be a senior individual within the business or an existing supplier. Fraudsters set up email accounts which are easily mistaken for genuine accounts, with minor spelling differences… often a corporate logo is copied into the email so that it looks genuine. The requests are often plausible : for example a purported seller sending a formal letter notifying details of their

EDITOR'S NOTE

In this quarter's newsletter we take a look at the need for companies and businesses to up their game as relates to the security of their data and online correspondence.

Over the past few years, there has been an increase in the hacking of websites and company databases exposing users to the risk of their identities/personal data being stolen and used to perpetrate crimes. Recently in 2014, the United States Company, Sony Pictures Entertainment, was hacked into and the personal data of a lot of its customers were stolen. It is therefore good that Section 22 of the Nigerian Cybercrime Act, 2015 provides for the offence of Identity Theft and Impersonation stating that a person who commits such offence will be liable on conviction to a 7 year imprisonment term or a N5, 000,000.00 fine or both.

It was recently stated by John Stewart, the Senior Vice President, Chief Security and Trust Officer at Cisco that: "This is not science fiction. It's a multibillion-dollar business of stealing intellectual property. We have got to be able to protect ourselves just that much better."

Cisco's Annual Security Report published on the 19th of January 2016 found that just 45 percent of organizations in the whole world are satisfied with their security position in the face of today's more sophisticated and resilient cyber-attacks.

The widespread hacking of company websites and databases also has negative implications for the companies. For example being data controllers it can expose them to fines or penalties for the breach of international data protection laws, such as the United Kingdom's Data Protection Act, 1998. Examples of personal data that can be used to perpetrate fraud include email addresses, email/computer passwords, contact addresses, bank details/records. This can be used in phishing emails and fake Outlook Web Access login pages in order to steal credentials, orthe creation of iOS malware to steal information, such as messages, contact lists, geo-location, pictures and voice recordings; and the exploitation of well-known software security vulnerabilities.

It is thus advisable to keep a security watch on all company websites and databases. The following can be done to achieve this aim:

1. Frequently up-date your operating system and application software to lower the risk of your computer being compromised;
2. Be cautious when downloading and installing software- there is always a risk that the software may have features that spy on the user, allowing unsolicited advertising or harmful software on your computer, especially if it is free or is not from a well-known and trusted brand.
3. Take care when opening unsolicited emails and do not click on any attachment or hyperlinks (especially shortened links) within them, you may end up being a victim of phishing attacks, because most of those links either open files loaded with malware or redirect to a site which may run malicious data on your computer.
4. Engage in sufficient due diligence. If an offer in an email appears too good to be

new bank accounts…" Hacker business models are also evolving. "If there is a way to make money illegally and through electronic techniques as the means, there is going to be somebody that thinks it up," said Stewart.One example is the use of stolen financial information to undercut an acquisition target's market value in order to later acquire the company at a fire-sale price. This tactic has been associated with Chinese hackers, said experts."If they are successful, they could drain the full value of the company — that's easily in the millions," said Rich Mason, president and chief security officer of cybersecurity consulting firm – culled from http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-

true or the prices on a website are ridiculously low or you receive a telephone call from an unknown person or company offering you some form of computer support, it is most likely a scam.

5. Hire a computer/software systems security expert.
6. Requests for money in an email should be verified with the sender in person, using the previously known contact details of the sender and not any new contact details provided in the email request. Preferable to responding to such an email, is to speak via telephone to a known person from the company that sent the email, and even better would be a physical meeting.
7. Frequent shredding of documents that are no longer in use especially those containing personal details of vendors or contractors.
8. Identifying emerging cyber threats and properly deciding which cybersecurity vendor to engage, is greatly enhanced when information is shared among companies and even with government agencies.
9. Use of anti-malware or anti-virus to prevent the compromise of employees' email accounts, because when an email is compromised, a hacker can use social engineering to get into a company's intranet and download files containing sensitive personal data.
10. Monitor employee behavior to security, to prevent complacency. Also look out for, identify and deal with any suspicious behavior on legitimate employee accounts.
11. Use Spam filter on email servers: This helps remove unwanted email from entering your users' inboxes and junk folders. Teach staff how to identify junk mail even if it's from a trusted source.
12. Use a comprehensive endpoint security solution in orderto prevent malware infections on user devices, examples are Antivirus, personal firewall and any intrusion detection device that ensures endpoint protection.
13. Maintain consistent security. Some antivirus programs update on a daily basis. Be sure that your software and hardware defenses stay up to date with new antimalware signatures and the latest versions. If you turn off automatic updating, set up a regular scan for all systems.
14. Practice good password formation with the use of a complex mix of characters. Also do not use the same password for different sites, bearing in mind also, never to write down your password.
15. Exercise caution when clicking on an attachment or links in an email that seems to come from your bank, or any other institution to avoid being taken to a harmful domain. It is better to log into your account directly than through the supplied link.
16. Sensitive browsing such as paying for travel ticket, banking or paying for other services should only be carried out on a device you own and a network you trust, this is to avoid one's data being copied or stolen.
17. Be careful with the device you plug in to your computer, malware and virus spread

via infected flash drives, smartphones and external drives.

18. Keep an eagle eye on your accounts because any suspicious activity that seems unfamiliar could be a sign that one's account has been compromised.
19. When you receive a call or email from an unknown person asking for personal details, simply respond with a decline to offer such information. It is best to physically visit the individual or company to verify authenticity, before parting with one's personal details.
20. It is best to use a less-targeted browser such as Google Chrome or Firefox.
21. When downloading a software, study carefully every write up throughout the installation wizard to avoid installing applications from unscrupulous download portals / vendors.
22. When downloading applications pay special attention to what permission each application is requesting, for instance it doesn't make sense for a weather application to be requesting access to one's photographs.
23. Layered security is key, back up all your data.
24. Use Familiar Websites: This means in carrying out research or even shopping, its best to start at a trusted site rather than using a search engine such as Google. Search engine results are often rigged to lead one astray, especially when you click on links that come up after the first few pages.
25. Be wary of misspellings on a website domain name or sites that use a different top-level domain (such as .net instead of .com), these sites often trick one into giving up their personal details.
26. A secure site for banking or purchase transactions must have an SSL (secure sockets layer) encryption installed. Such sites' URL start with HTTPS:// (instead of just HTTP://), in addition an icon of a locked padlock appears either in the status bar at the bottom of your web browser, or next to the URL in the address bar, depending on the browser one is using.

Finally, the above list is not exhaustive. Inasmuch as hackers keep devising new creative methods of cybercrime and hacking, we the online users must exercise caution in our online activities and interactions in other not to become victims of breach of cyber security.

The GOS Newsletter has been prepared for clients and professional colleagues as a general guide to the subject matter.It is not meant to substitute specialist legal advice about your specific circumstances.

G.O Sodipo and Co disclaim any liability for the decisions you make based on this information.

Please let us know if you would like to discuss any issue in more detail;

E-mail: b.sodipo@gosodipo.com

All Photo Credits: Google Search Engine.

“One should approach online transactions and correspondence with utmost caution, being on guard against possible deception”-Barrister B.V Enwesi,LLB,BL,LLM(E-commerce Law)

G.O SODIPO & CO
Tel: 08023198641

E-mail:
We're on the Web!
www.gosodipo.com

G.O SODIPO & CO
Tel: 08023198641

E-mail:
We're on the Web!
www.gosodipo.com