How do you Spend your Time at Work?

Based on a Forbes article: Wasting Time At Work: The Epidemic

According to the 2014 data from Salary.com, who conducted a survey amongst 750 employees on how they spend their time at work it was found that employees wasted even more time than the year before (2012-2013).

In the previous year, 69% of employees admitted that they waste time at work on a daily basis. The latest survey has found that the number of employees that now admit to wasting time at work on a daily basis, has increased to 89%. They are now spending longer periods on "wasting time." The statistical breakdown on wasted time is as follows:
•31% waste roughly 30 minutes daily
•31% waste roughly 1 hour daily
•16% waste roughly 2 hours daily
•6% waste roughly 3 hours daily
•2% waste roughly 4 hours daily
•2% waste 5 or more hours daily

According to Salary.com, contributor Aaron Gouveia, 4% of employees surveyed wastes at least half the average workday on tasks that has nothing to do with their actual job.

In another survey conducted by Harris HRS, Poll for CareerBuilder surveyed 2,138 hiring managers and HR professionals and 3,022 full-time workers across a range of industries and companies to determine the reasons for the increased wasting of time. The use of technology is the leading cause for time wasted. Twenty-four percent of workers admitted that they spend at least an hour a day on personal email, texts and personal calls. The survey results reflects that the time wasters are keeping themselves busy with the following:

1. Talking on the cell phone and texting – 50%
2. Gossiping – 42%
3. Surfing the Internet – 39%
4. Spending time on Social media – 38%
5. Taking a snack break or smoke breaks – 27%
6. Being distracted by noisy co-workers (in open plan office)– 24%
7. Attending meetings – 23%
8. Spending time on email – 23%
9. Being distracted by co-worker dropping in – 23%
10. Being distracted by co-worker calls on speaker phone (in open plan offices) – 10%

Employers also shared some of the real-life examples of what they've seen employees do when they should have been focussing on work:
•A married employee was surfing a dating web site and then he denied it while it was still on his computer screen;
•An employee was caring for her pet bird that she smuggled into work;
•An employee was shaving her legs in the women's restroom;
•An employee was lying under boxes to scare people;
•Employees were having a wrestling match;
•A sleeping employee claimed he was praying;
•An employee was changing clothes in a cubicle; and
•An employee was printing a book from the Internet.

The question is can the employer do something about it? How can one manage?
According to Cheryl Conner, employers can actually do something about this, which, under normal circumstances should already be workplace practice.

1. **Better workplace policies:** which deals with excess noise, speakerphones and continual drop-byes. In open plan office this will always be a problem and in some modern buildings there are areas where employees can take tea brakes according to set times. However, most people do not even know that they are noisy and loud and forums for these discussions should be in place to address the problem. Therefore an employee conduct policy, which allows for discussion around the challenges and expectations of the team and organisation might be sufficient to curb the fore mentioned practices. However, a policy to remove personal devices or forbidding all access and texting during working hours is likely to be resented or simply ignored, as many will claim that they need the device to conduct their work.

2. **Flexible working agreements:** Google set the trend to put emphasis on work accomplished instead of hours served. This practice places trust and accountability on the shoulders of workers while allowing flexibility for the non-work activities that if kept within bounds can ultimately keep a worker refreshed and productive. When an employee completes a project and then goes home, that employee is less likely to waste their time by keeping others from performing their tasks. Many workers (and millennials in particular) are more productive if they are allowed to work for a period of time, then take a break to play a game of ping pong or browse social media for a few minutes in between performing segments of work.

3. **Internet filtering**. Allows for Access controls by keeping users off sites that could cause a data breach and protect the business from the legal liability that comes with a data breach. It also improves workforce productivity and allows for site blacklisting and automatically enforces browsing policies that keep users off non-work related sites like gaming or social media and dating sites. The use of time-based browsing policies modifies blacklist rules to allow employees to visit non-work sites outside of standard business hours.

4. **Education**. Employees may be unaware of the implications of using the organisation's time for activities such as talking badly about the organisation, being disrespectful about its customers, or gossiping about fellow employees, specifically when they are carrying out these activities online. Being caught is easier than one would think. These activities can result in a negative job review and some situations are severe enough to end a career. Employees should be educated on these issues. It is guaranteed that activities on the Internet will not stay private and one should be aware that whatever you share with a recipient/s can go viral. Therefore it would be wiser to concentrate on your job before embarking on a gossiping spree and being very belligerent about your organisations business.

In conclusion a code of good conduct should be developed by organisations through utilising change management principles, whereby all employees are involved during the development. Therefore they will be in agreement on how to manage wasting time and dealing with unsuitable work practices.

Resources:
Contributor Cheryl Conner
Contributor Aaron Gouveia
Forbes' Entrepreneur Newsletter

THE 'DARK SIDE OF THE NET' ARTICLE SERIES: Part Four

Dr Marcus Leaning
Senior Fellow
School of Media and Film
University of Winchester, Winchester, United Kingdom
eMail: marcus.leaning@winchester.ac.uk

and

Udo Richard Averweg
IT Project Manager
Information Management Unit
eThekwini Municipality, Durban, South Africa
eMail: udo.averweg@durban.gov.za

Professor Marcus Leaning
School of Media and Film
University of Winchester, Winchester, United Kingdom
eMail: marcus.leaning@winchester.ac.uk

and

Udo Richard Averweg
IT Project Manager
Information Management Unit
eThekwini Municipality, Durban, South Africa
eMail: udo.averweg@durban.gov.za

Introduction

This article is the fourth in a series that considers what we may term the 'dark side of the net'. Our series looks at a number of practices and activities on the internet that either verge on the illegal or are illegal. Such practices and activities can have serious consequences for how organisations function and we discuss these in the hope that readers may have their awareness and understanding of these issues reinforced.

In our first article, published in the December 2016 edition of the *Journal of the Southern African Institute of Management Services*, we discussed the activity of spam. In our second article, published in the March 2017 edition of the same journal, we discussed the practices and activities of hacking. In our third article, published in the June 2017 edition of the journal, we focused our attention on bitcoin and crypto currencies. In this fourth (and concluding) article in the four-part series, we discuss the fora and forums of, and available services on the dark side of the net.

The dark net: its fora and forums

In July 2017 the dark net market place *AlphaBay* was taken down by co-ordinated law enforcement activities in a number of countries. Subsequent to this take down, the users of the services sought alternative venues to continue their buying and selling of drugs and other illegal merchandise. Many of them moved to an alternative venue, *Hansa*. Unbeknown to them *Hansa* had, two months previously been taken over itself by law enforcement agencies and it was operating as a trap to ensnare users once they had fled *AlphaBay*.

We now consider some of the means by which information and communication on the dark net is hidden from the 'surface' or normal web; and one of the main uses of the dark net - the trading in problematic and illegal goods.

The fora of the dark net

The dark net is a broad term that is applied to a range of communicative practices and virtual spaces that lie outside the normally experienced web and social media pages the vast majority of internet user's experience. The content and the communication that takes place on the dark net is not specifically illegal – though a high degree of it is – as it also encompasses communication and practices that participants wish to remain private and not public knowledge. Though some authors have used the term dark net to refer to a wide range of practices that occur both through common place internet services and the 'hidden' systems (Bartlett, 2014) here we limit our discussion to those systems that require explicit software to reach. It is also necessary to disaggregate the dark net or web from the deep web or net.

The deep web is those web pages that are not indexed and cannot be found with a normal search engine. The deep web is vast - with estimates ranging from it being 20 to 100 times the size of the searchable web. It consists of information that resides behind firewalls, that is on pages that are not linked or indexed or pages that are dynamically created by queries from web forms to databases as well as many other systems. Much of the information in the deep net is widely used and we do encounter it on a regular basis – pages from various web interfaces such as expedia.com reside in the deep web, we cannot search for these pages through normal search engines and they are not indexed but can be reached though entering queries into specific web interfaces.

The dark net can be understood as a subset or category of the deep net. As such we can demarcate the dark net from other forms of communication and data. For our purposes we identify the dark net as a specific section of the deep net that cannot be readily access through search engines. It is not a hidden part of the normal web, such as a secret Facebook group but a specific approach to hiding information and making the identity of the users of that data difficult to identify.

Here we will describe the methods by which the dark net can be reached and some of the forums that exist there.

Reaching the dark net – TOR

Dark net web sites are typically accessed using TOR (The Onion Router) – a technology that involves covering network traffic with layers of encryption and then routing the data through multiple network pathways which continually shift.

The TOR technology allows users to visit web pages anonymously and to circumvent attempts to restrict access to particular sites. It is used by dissidents, journalists and others who wish to communicate anonymously for fear of having their messages intercepted by state agencies. As well as being used in the United States of America, Europe, South Africa and other democracies, TOR is used by anti-government actors such as human rights activists in countries such as the People's Republic of China, the Syrian Arab Republic and Iran. TOR was developed by the United States (US) Naval Research Laboratory and was released under a free license in 2004 and then received backing from the Electronic Freedom Foundation. Because TOR is used by numerous anti-systemic groups which the US government has an interest in supporting, it continues

to be in part funded (about 60%) by the US State Department and US Department of Defense (Greenwald, 2013).

TOR operates by having numerous computers functioning as nodes. These nodes can relay traffic between them. Once information is sent to the TOR network it is relayed across numerous nodes on its way to its destination. Traffic that is intercepted on the network is heavily encrypted multiple times. Moreover, the data has had both its origin and destination information removed and so is very difficult to trace.

From a client perspective, the TOR system is a browser that can be installed upon any Mac, PC or Linux machine – indeed the browser is a version of the *Firefox* browser. Once the TOR Browser Bundle has been downloaded and installed, the user enters addresses as they would any other web page. However, sites on the TOR network are not reachable via a normal browser and the addresses are constituted differently from normal web addresses and make use of a special top level domain – onion. TOR addresses consist of a string of 16 (seemingly) random numbers and letters with the suffix onion/. For example, http://4u3ptawty2mn53bz.onion/ (this is a fake address). The actual address is the hash produced by public key encryption when the hidden service to which it points is initially established.

Due to the various sites and services available on the dark net / TOR system being unindexed and unsearchable using normal web searching technologies, alternative systems have evolved. There are various search engines for the dark web (only reachable using the TOR browser) and a number of hidden wikis.

Available services
The services available on the dark net can be grouped into a number of different categories, such as markets, sharing media files, and communication and community.

Markets
There are numerous market places offering a vast array of services and goods. Historically one of the most famous dark net systems was the *Silk Road* – a site launched in February 2011 that was most famous for selling illegal narcotics. The site allowed users to buy and sell virtually any item but was best known for selling drugs in exchange for bitcoins. Allied sites such as *Armoury* sold guns and other weapons.

The *Silk Road* was closed down in October 2013 after the FBI seized control and impounded all the bitcoins in members *Silk Road* wallets (members had to load bitcoins onto a site specific wallet to purchase or sell items) (Clark, 2013). Following its closure and prosecutions of a number of the operators (who all worked under the pseudonym of the *Dread Pirate Roberts* (the name of the figure-head pirate who was role played by different people in the film *The Princess Bride*)) the *Silk Road* re-emerged as the *Silk Road 2* and was also closed down (in 2014).

A *Silk Road 3* emerged during 2016 but was unconnected to the original and seemed to have been established to defraud users. As with other market places the *Silk Road* allowed users to buy or sell virtually any goods anonymously.

In addition to the selling of illegal drugs there are also market places for stolen credit card numbers, stolen goods, fake passports, guns and weapons, counterfeit money, hacking software, stolen software and other media content. Services such as the laundering of bitcoins, hacking and even assassination (though there has been considerable scepticism about whether this service was ever real or simply scams) are also proffered

for sale on various market places. *AphaBay* and *Hansa* are both examples of this such markets.

Markets on the dark web are unregulated and there is little recourse for buyers and sellers who are deceived. One innovation to remedy the problem of untrustworthy traders and vendors is the use of reviews in a similar way to other more legitimate web markets. Thus purchasers of drugs, fake passports and guns are able to offer a review of the service they receive and thus advise other customers of the reliability of the service.

Sharing media files

There are numerous sites for the sharing of media files. These include commercial films and television series that have been stolen or illegally copied, large quantities of various forms of pornography and software. Such sites make use of various additional technologies and practices to share files. These include bit torrents and sharing systems such as virtual private networks that use TOR technology to allow users to share files without risk of interception.

The system *OnionShare* was developed after investigative journalist Glenn Greenwald's partner, David Miranda, was detained at Heathrow Airport under suspicion for transporting 58,000 documents (on a USB pen drive) which he had gained from Edward Snowden. Micah Lee, a staff developer with Greenwald's organisation, developed the system so that documents could be transferred without possible interference from third party agents (Crawford, 2014). Similarly Wiki leaks, the site established by Julian Assange to facilitate the release of government documents, can be found on the dark net.

Communication and community

In addition to the commercial exchange and sharing of information, the dark net facilitates various forms of communicative spaces such as forums, blogs and secure email services. The secure email services draw heavily upon privacy and encryption software and a number of email systems are available.

As we noted earlier in this article, it is necessary to disaggregate the dark web from the deep web – the dark web forms part of the deep web. It should be noted that these terms are not something new – their first conflation was already some eight years ago.

Some concluding remarks

In 1989 the British computer scientist, Sir Tim Berners-Lee, invented the world wide web (an Internet-based hypermedia initiative for global information-sharing), he could not have predicted the emergence of the dark side of the net a few later years.

While nowadays the dark side of the net has both 'light' and 'dark' sides to it, in this article series we have endeavoured to discuss some of the current practices and activities on both sides of its light-dark spectrum. We hope our discussion has achieved this so that organisations may realise the consequences some of these practices and activities. We also trust that readers of this journal have had their awareness and understanding of these issues reinforced. This then concludes our four-part article series.

Further reading

Bartlett, J. (2014). *The Dark Net*. London: Random House.
Clark, L. (2013, 9 October 2013). A guide to the Silk Road shutdown. *Wired*. Retrieved from http://www.wired.co.uk/article/silk-road-guide

Crawford, D. (2014). *Onionshare: the 100 percent darknet file sharing app*. Retrieved on 4 September 2017 from https://www.bestvpn.com/onionshare-the-100-percent-darknet-file-sharing-app/
Greenwald, G. (2013, 4 October 2013). NSA and GCHQ target Tor network that protects anonymity of web users*. The Guardian*. Retrieved from https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption