Cyberint

Social Media

a Growing Risk for Corporate Security

Introduction

Organisations are spending a growing amount of cash on cybersecurity while cyber crime continues to grow.

Last year, Gartner estimated that the global spend on security in 2016 was around US$80 billion, an increase of roughly five per cent over the previous year. According to Forbes magazine, cyber crime costs business as much as US$500 billion a year. Juniper Research predicts that this figure is likely to more than quadruple over the next four years bringing the total cost of data breaches to US$2.1 trillion by 2019.

The cyber criminals' growing success in breaching corporate cyber defences is partly underpinned by society's increasing reliance on social media. Companies use social media networks for marketing and brand recognition. Executives use them for job search and professionals use them to exchange ideas and establish new contacts. All of which makes them rich hunting grounds for cyber criminals.

A new and sinister profession, 'social engineering', has grown up around harvesting these vast amounts of personal data for criminal purposes. Social engineers manipulate social media to provide enough personal data on key individuals in targeted organisations to perpetrate carefully orchestrated frauds across a wide variety of sectors.

And while corporate spam filters may block some unsolicited emails carrying dodgy links, corporate executives and people holding key positions are only too willing to freely open links in Twitter, Facebook or LinkedIn, especially when they have been socially engineered to appear to come from a trusted source.

Cyber crime costs businesses as much as $500 bil. a year

Cyber criminals have now developed the art of creating links to apparently innocuous web pages which host phishing campaigns and may even invisibly inject malware into the victim's device, potentially opening up their organisation's entire IT system to a successful cyber attack.

The consequences can be dire. Companies can quickly discover that their most confidential data and customer details are in the hands of their competitors or being sold on Dark Web forums where illicit goods and services are traded anonymously.

Businesses have yet to wake up to the true level of risk posed by social media. Few have any safeguards in place, while encouraging a bring your own devices to work (BYOD) policy. This means that staff are using the same devices to access the corporate IT network while simultaneously using them for their own personal social networking.

Unless companies come to realise that their security perimeters must grow beyond the corporate firewall to encompass social media networks and other areas such as the Dark Web, then the global cost of cyber crime will continue to mushroom.

The Rapid Growth of Social Media

The historically unprecedented impact that social media is having on all of us extends to every aspect of modern life. Today, social networks such as Facebook, LinkedIn and Twitter are driving new forms of social interaction, dialogue, exchange and collaboration.

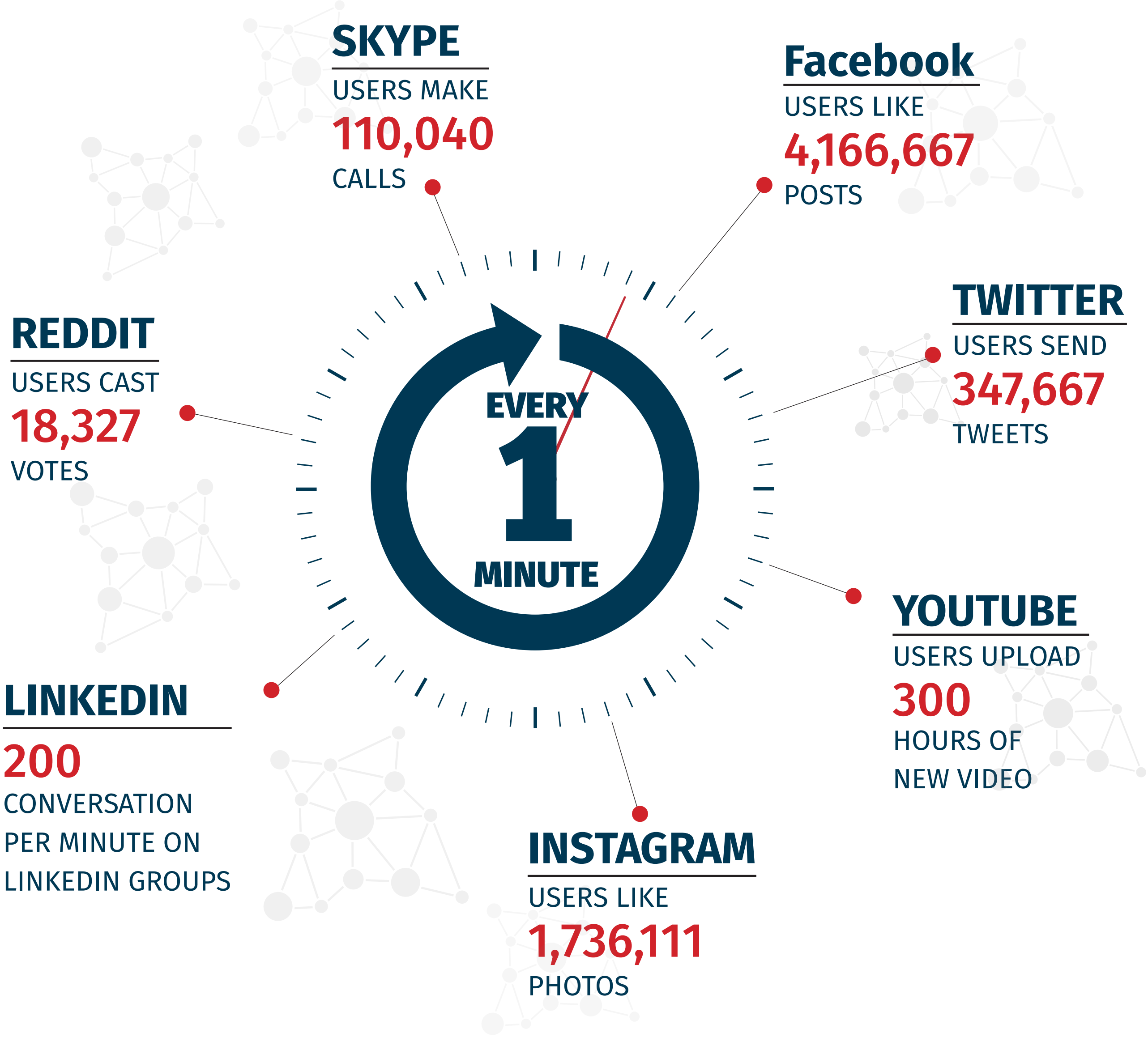
Social networking websites now represent some of the largest communities on the planet. As of the fourth quarter of 2015, Facebook had 1.59 billion monthly active users, more people than the population of China, which is roughly 1.38 billion. Twitter has 240 million active monthly users. And, although LinkedIn, the social network for professionals, has only around 100 million monthly active users, many of its members occupy key positions or are high net-worth individuals.

> **Facebook has 1.59 billion monthly active users, more people than the population of China**

Social networking sites (referred to more broadly as Social Media) enable users to swap ideas, post updates and comments, and participate in activities and events, while sharing their wider interests. From general chat to propagating breaking news, from scheduling a date to following election results or coordinating disaster response, from gentle humor to serious research, social networks are now used for a host of different reasons by various user communities

In business, Social Media has changed the way organizations of all types and sizes are conducting communications. Social media is an increasingly preferred vehicle for organizations to interact with internal and external stakeholders: organizations are using social media tools and ‘big data’ platforms to build brands and communities which can engage customers in regular feedback dialogues; HR managers look for job candidates on LinkedIn; marketers are initiating campaigns on social networks; and technical support personnel use Twitter as a platform to discuss and announce critical issues in real time.

But the very ubiquity of social media, its speed of growth and the increasing reliance individuals place on it make it a target for organised cyber crime.



EVERY 1 MINUTE

SKYPE
USERS MAKE
110,040
CALLS

Facebook
USERS LIKE
4,166,667
POSTS

TWITTER
USERS SEND
347,667
TWEETS

YOUTUBE
USERS UPLOAD
300
HOURS OF
NEW VIDEO

INSTAGRAM
USERS LIKE
1,736,111
PHOTOS

LINKEDIN
200
CONVERSATION
PER MINUTE ON
LINKEDIN GROUPS

REDDIT
USERS CAST
18,327
VOTES

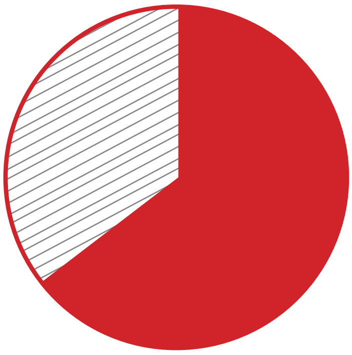
Social Networks Used to Breach Corporate IT Systems

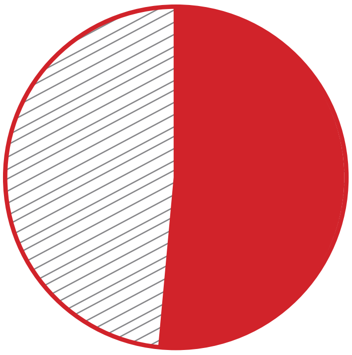
Most organisations have been blindsided by cyber criminals' rapidly growing use of social media such as Facebook, LinkedIn and Twitter as a way of infiltrating corporate IT systems in order to steal confidential data. According to PWC's 2015 Information Security Breaches Survey, 13% of large organizations had a security or data breach in the last year relating to social networking sites.

13%
of large organizations had a security or data breach in the last year relating to social networking sites.

And while companies are increasingly aware of the need to safeguard their IT systems from cyber crime and espionage, only a small proportion of organisations are doing anything to counter the threat posed by malicious manipulation of social media. According to a report by Websense on social media security risks, 63% of respondents agree that employee use of social media puts their organizations' security at risk, but only 29% say they have the necessary security controls in place.

63%
of respondents agree that employee use of social media puts their organizations' security at risk





Over 51 per cent of UK organizations do not address social media risk as part of their risk assessment process, with 45 percent indicating that they have no plans to do so in the coming year. Of those that do address social media risk, 84 per cent rated their organization's social media risk-assessment capability as "not effective" or just "moderately effective."

Over 51%
of UK organizations do not address social media risk as part of their risk assessment process

As companies have been increasing their cybersecurity spend over recent years, many now have relatively well secured IT systems together with effective security protocols. But while an organisation's firewall might be secure, the growth of social networking has left most organisations with an exposed flank.

The information now residing in social networking websites is a virtual goldmine for cyber criminals and online fraudsters. Few people have any real grasp of the risks they take when interacting on social media or the size of the digital footprint they leave behind them. According to Consumer Reports' survey, fifty-two percent of adult users of social networks such as Facebook have posted risky personal information online.

Facebook, LinkedIn and Twitter are huge repositories for personal information on billions of users. This has spawned a new form of data mining known as 'social engineering', which involves garnering all the information on a specific individual with a view to exploiting this knowledge by targeting the individual with a scam that has been tailored around them. Alternatively, a social engineer who is active on social networking websites may be searching for a key individual working at an organisation that has been targeted by organised cyber criminals.

According to the FBI, criminals are using data posted on social networking websites to garner information on individuals who have been targeted for 'spear phishing' attacks targeting multiple industry sectors.

In spear-phishing attacks, cyber criminals target victims because of their involvement in an industry or organization they wish to compromise. Once the online social engineers have gathered enough data on a member of the company, the cyber criminals will typically create fake emails purporting to come from an executive at the targeted organisation. Often, the e-mails contain accurate information about victims obtained via a previous intrusion or from data posted on social networking sites. This information adds a veneer of legitimacy to the message, increasing the chances the victims will open the e-mail and respond as directed.

Information can be actively extracted from a victim, for example through Elicitation; The use of conversation to extract information from people without giving them the feeling they are being

> **Elicitation; The use of conversation to extract information from people without giving them the feeling they are being interrogated.**

Click-Jacking Scams

Spear phishing attacks are not the only threat. Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions such as downloading malware. Numerous click-jacking scams have employed “Like” and “Share” buttons on social networking sites. A common vulnerability in Social Media is derived from the usage of weak authentication mechanisms, usually a basic password authentication. The commonly used account recovery mechanisms, such as challenge questions are easily defeated. MIT researchers found that there is a 17% chance of guessing the answer.

CyberInt researched 25 Fortune 500 companies over the last four years, examining a total of 800,000 Tweets and 50,000 Facebook comments and posts. The research showed that 1.92 per cent of all posts, comments and Tweets that included URLs in them were malicious or attempted attacks. Twitter represented by far the major threat, with 95 per cent of the malicious URLs found in Tweets and only 5 per cent in Facebook posts and comments. Of the malicious Twitter URLs, 98 per cent were used for phishing schemes and the remaining two per cent were attempts at malware drop-offs.

Cyber Espionage

A common danger stems from over sharing of information, which is eagerly gathered up by business rivals and, in the case of some industries, foreign powers. People have become increasingly open online – posting information about their lives through status updates, location check-ins and hashtags. In a Forrester Research survey last year of more than 150 companies that monitor social media, more than 82 percent said they use this data for competitive intelligence — the most cited reason for the monitoring. With good reason: A single insider’s Twitter Inc. post can be more valuable than a stack of analysts’ research.

Companies that monitor social media, more than 82% said they use this data for competitive intelligence

Bot Activity

Some cyber criminals use 'social bots' - software designed to mimic human communication - to create fake social networking identities. Apart from spreading malicious links, Bots' abuse of social media can be manifested in automated bot activities. Chat bots are being used to social-engineer the victim into clicking the malicious links. Several malware samples that appeared recently have used social media for C&C.

Fake Facebook Pages are Flytraps for the Unwary

Sometimes, the cyber criminals post fake Facebook pages to elicit personal details. As the links to these pages can be spread virally, they are essentially a scatter gun approach to social engineering. They can, however, also be sent to targeted individuals in the hope they might open them.

Facebook has recently been struck by an epidemic of Facebook pages showcasing fake ads mimicking those of major brand names. But behind the offers of free international flights or a lifetime's supply of hamburgers lurk cyber criminals hungry to garner enough personal information to defraud those unlucky enough to have visited the bogus Facebook pages or to steal their online identities.

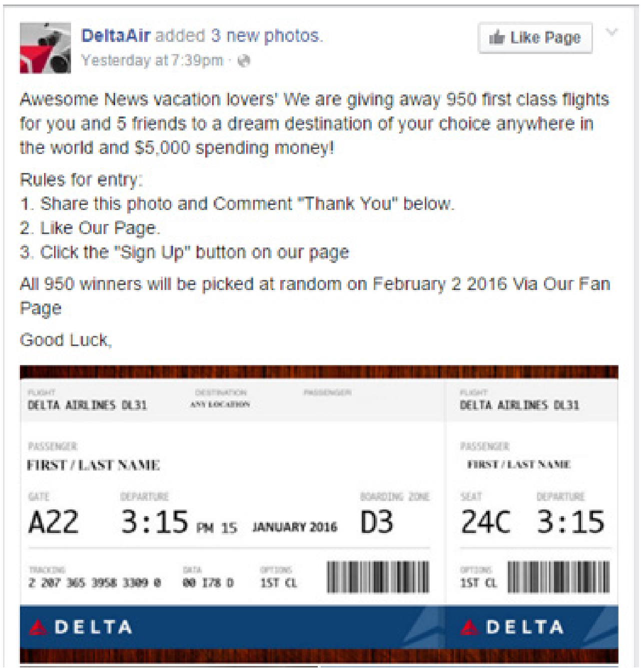
Delta Airlines is the latest corporate brand to be tarnished. For the third time in less than a year, Delta Airlines and thousands of its customers have been hit by a Facebook phishing scam. The latest scam lasted for three days in the last week of January this year and netted the perpetrators the personal details of at least 35,500 visitors to the bogus pages. The scam was discovered by CyberInt during a routine trawl of a variety of social media networks. At least two Facebook community pages carried what, at first glance, appeared to be genuine ads from Delta, encouraging visitors to share a photo with friends or to sign up for promotional deals. A third bogus page offered "Delta Airlines Gift Bags full of amazing prizes! Five first-class tickets to anywhere in the world, $5,000 in cash and a Delta key chain."

The latest Delta scam follows hard on the heels of other major brand scams which have been posted on Facebook over the last month. A fake page carrying an ad for the hamburger chain McDonalds in celebration of its 61st anniversary appeared to offer visitors to the page a lifetime of free meals; all they had to do was to fill in some personal details in order to register.

Fast food chains Kentucky Fried Chicken and Wendy's Hamburgers have also been targeted this year with similar offers of a "lifetime pass" for free food. US grocery chain Trader Joe's has also been the subject of a similar Facebook scam in the last few weeks.

Judging by previous similar scams, the most likely scenario is that online fraudsters will use the email addresses of the people who liked the pages or shared them may soon be victims of 'phishing scams'.

These could, for instance, be bogus offers of cheap flights designed to make fraudulent payments. Those who have filled in their bank or credit card details may suffer immediate financial loss. Disturbingly, "phishing scams" could also illicit travel details such as passport numbers and expiry dates, enabling identity theft.



DeltaAir added 3 new photos.
Yesterday at 7:39pm ·

Awesome News vacation lovers' We are giving away 950 first class flights for you and 5 friends to a dream destination of your choice anywhere in the world and $5,000 spending money!

Rules for entry:
1. Share this photo and Comment "Thank You" below.
2. Like Our Page.
3. Click the "Sign Up" button on our page

All 950 winners will be picked at random on February 2 2016 Via Our Fan Page

Good Luck,

Summary

Most companies are blind to the significant and now growing threat to their security posed by the manipulation of social media. As human error is the hardest thing for any organisation to guard against, companies are increasingly vulnerable to attacks emanating from social media,

While using social networking sites to exchange ideas, make new contacts and share information may bring real benefits, it also carries huge risks, not only for the individual concerned but also for the organisations they work for.

Cyber attacks not only put companies at risk from major frauds. They also expose organisations to compliance violations, reputational loss, sensitive data exposure, loss of customers' trust and worse.

Some cyber breaches are designed to inject ransomware, which is designed to lock up an organisation's most sensitive data, only releasing it when a hefty ransom is paid.

A major US hospital in Los Angeles, the Hollywood Presbyterian Medical Centre, located in the heart of LA, was, for example, hit by such a ransomware attack in mid-February of this year. The hackers reportedly demanded over 9,000 bitcoins, roughly US$3.6 million, in order to release encryption keys to computer systems they had hijacked holding patient data, X-Ray scams and ground-breaking lab research

The rapid growth of social media and our increasing reliance on it has opened up a whole new front in the war against cyber crime. So far, the cyber criminals are winning. In order to defend themselves, organisations must now take steps to secure the outer perimeter of their cyber defences, taking full account of the growing threat posed by the rapid development of social media.

Cyberint
Protection Beyond the Perimeter

United Kingdom
Tel: +442035141515
sales@cyberint.com
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +972-3-7286-777
sales@cyberint.com
3 Columbus Circle | NY 10019 | New York | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
sales@cyberint.com
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
sales@cyberint.com
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com **www.cyberint.com**