dte business advisers

- Business Advisory & Audit
- Tax Consultancy
- Corporate Finance
- Forensic Accounting
- Outsourcing & Payroll Management
- Financial Planning

UPDATE ON CYBER SECURITY

Richard Bell MAAT FCCA

Partner & Head of IT Support

November 2019

About Richard…

In addition to audit, Richard leads the outsourcing of the finance function for a number of clients. Richard also has experience in dealing with the UK subsidiaries of overseas companies.

Richard, a Fellow Chartered Certified Accountant, provides a proactive, straightforward approach to advice and has built up long term relationships with clients and has extensive experience across a broad range of sectors.

Richard is also Head of IT Support at DTE.

Specialisms: audit and accountancy, business advisory, outsourcing

What is cyber security?

Cyber security is defined by the ‘National Cyber Security Centre’ how individuals and organisations reduce the risk of **cyber attack**.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access - both online and at work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices, and online.

Why is it important?

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

The 5 most common cyber attacks in 2019

Cyber attacks are on the rise. 32% of businesses have identified cyber security breaches or attacks in the past 12 months, according to the UK government’s Cyber Security Breaches Survey 2019.

But how do these attacks manifest themselves, and what are the most common cyber threats to organisations today?

In this post, we explore some of the most common cyber attacks and discuss what you can do to protect your organisation.

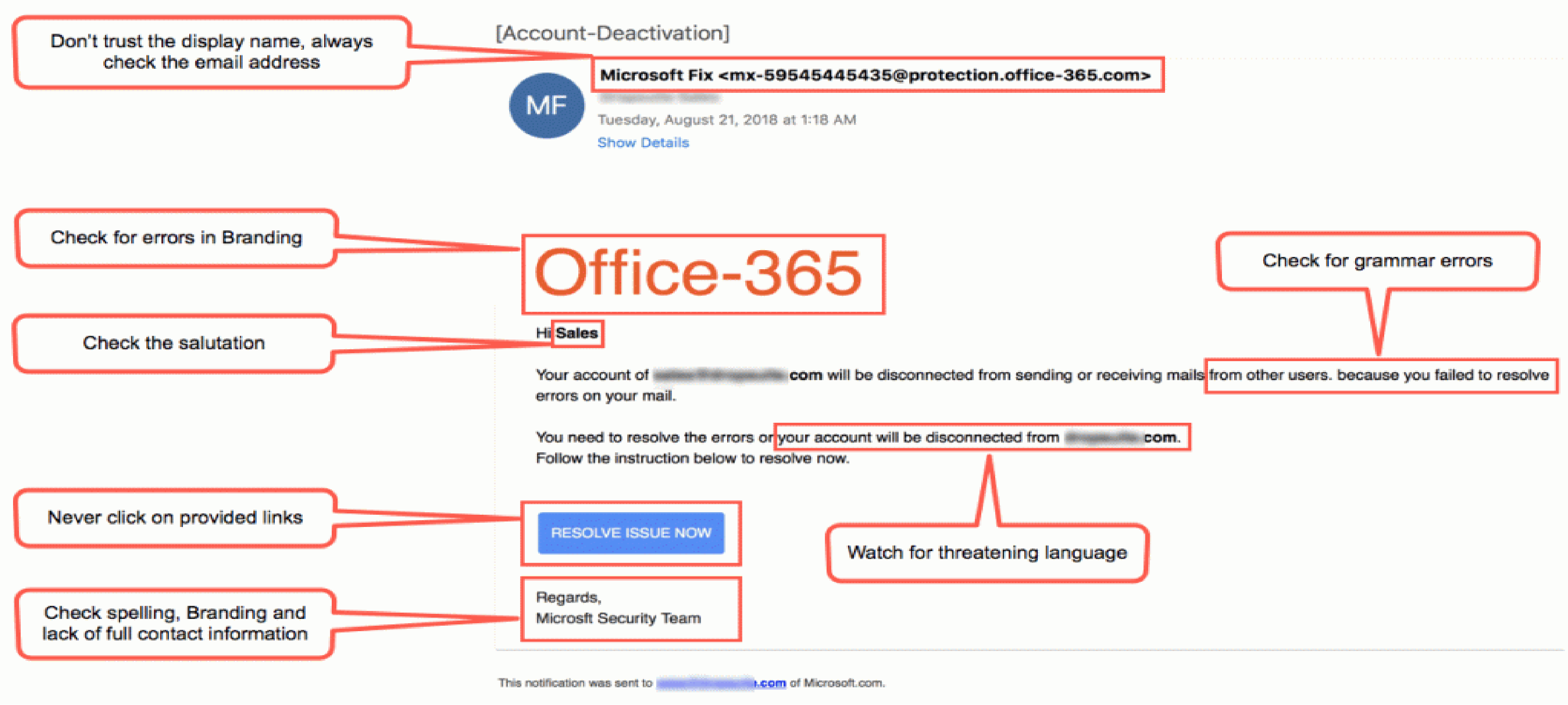
1. Phishing

What is phishing?

Phishing is a broad term for any attempt to trick victims into sharing sensitive information such as passwords, usernames, and credit card details for malicious reasons. Phishing tries to trick users into clicking a malicious link or downloading an infected attachment or divulging sensitive or confidential information.

Proofpoint's 2019 State of the Phish Report found that 83% of respondents experienced a phishing attack in 2018 (up from 76% in 2017), and Verizon's 2019 Data Breach Investigations Report revealed that 32% of data breaches involved phishing

Phishing – What to look out for



[Account-Deactivation]

Microsoft Fix <mx-59545445435@protection.office-365.com>

MF

[redacted]

Tuesday, August 21, 2018 at 1:18 AM

Show Details

Office-365

Hi **Sales**

Your account of [redacted] **com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from [redacted] **com**. Follow the instruction below to resolve now.

RESOLVE ISSUE NOW

Regards,
Microsft Security Team

This notification was sent to [redacted].com of Microsoft.com.

Don't trust the display name, always check the email address

Check for errors in Branding

Check the salutation

Never click on provided links

Check spelling, Branding and lack of full contact information

Check for grammar errors

Watch for threatening language

dte business advisers

www.dtegroup.com

Types of phishing

There are many types of phishing, including:

Vishing: Voice phishing or ‘vishing’ is a type of phishing conducted by phone. Most vishing attempts try to get the victim to reveal information like PINs, payment card details and passwords. Criminals then use those details to access online accounts to steal information or money.

Smishing: SMS phishing or ‘smishing’ is becoming a more popular form of phishing, partly because we increasingly rely on smartphones in both our work and personal lives.

Spear phishing: Spear phishing is a targeted form of phishing attack – usually conducted to seek financial gain or obtain insider information – where cyber criminals adapt their methods to reach a specific victim. Spear phishing attacks are rarely random – instead, they are most often conducted by perpetrators seeking financial gain or insider information.

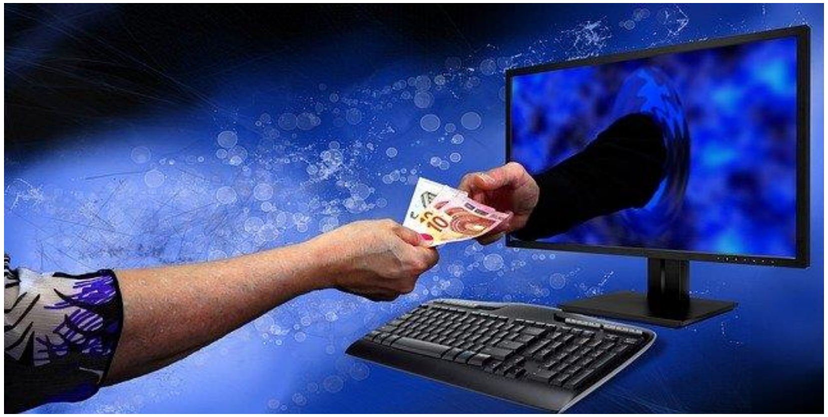
Beware of posting personal information on social media sites etc
Beware of sending sensitive details by unecrypted email
Don’t click on links in emails e.g. email from bank – look up telephone number and check or independently go to website
Use common sense – why would a friend be randomly looking for personal information?
Invoices Fraud - emails being intercepted and bank details being amended
Conveyancers – ‘Friday Afternoon fraud’
CEO Fraud

2. Ransomware

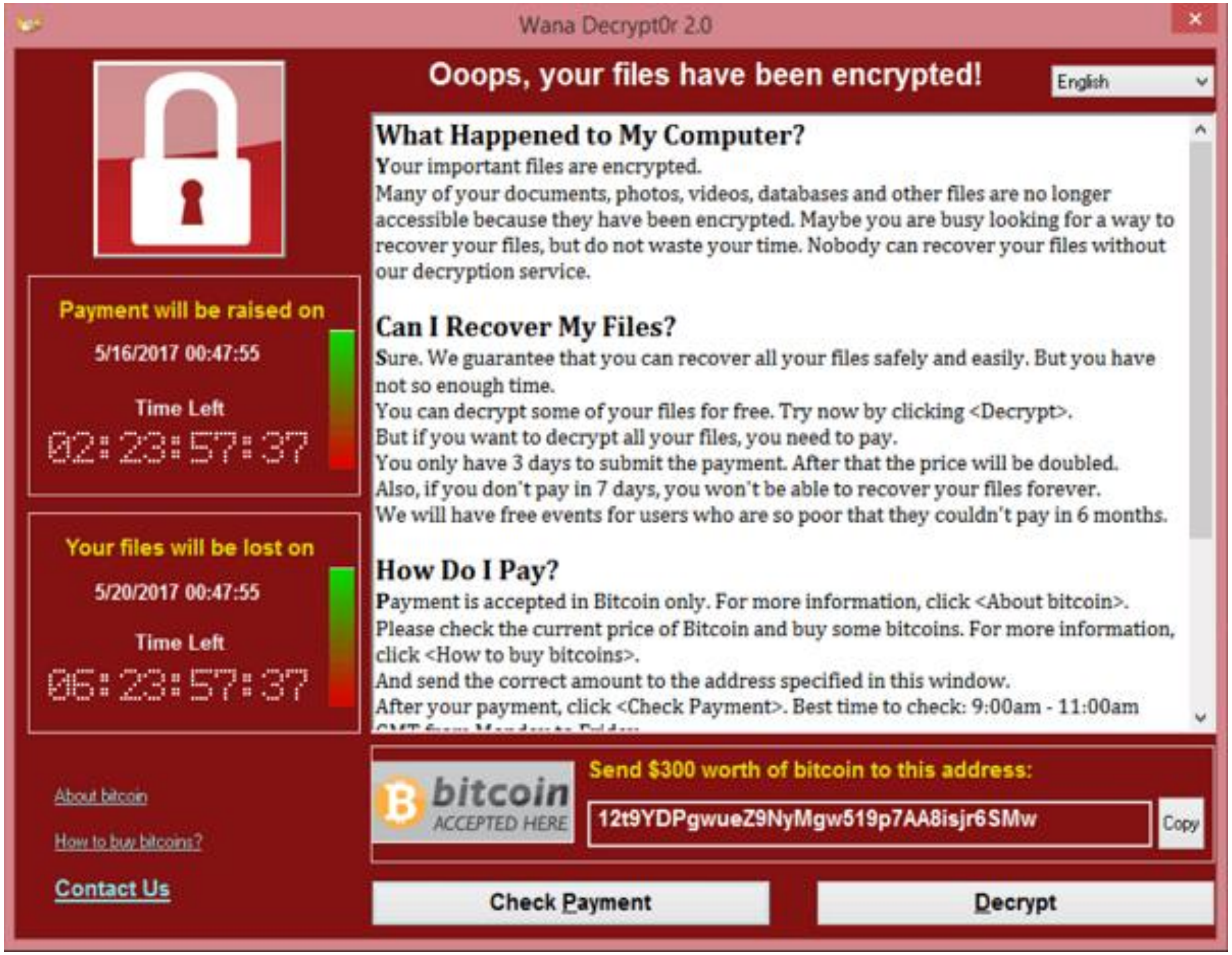
What is ransomware?

Ransomware is a type of malicious software designed to deny access to files until, or threaten to publish the victim's data unless, a ransom is paid (although there is no guarantee that access will be restored, or that the criminal hacker will destroy the data).

The threat is growing. The 2019 Official Annual Cybercrime Report predicts that a business will fall victim to a ransomware attack every 14 seconds in 2019, and every 11 seconds by 2021.



Ransomware – an example



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

3. DDOS ATTACKS

What is a DDoS attack?

A DDoS (distributed denial-of-service) attack attempts to disrupt normal web traffic and take a site offline by overwhelming a system, server or network with more access requests than it can handle.

DDoS attacks typically serve one of two purposes:

1) An act of revenge against an organisation.

2) A distraction that allows cyber criminals to break into the organisation while it focuses on restoring its website.

Help fund our people powered movement.

Donate now.

DDOS ATTACKS – How to prevent it

The reputational and financial damage as the result of the service unavailability inflicted by a successful DDoS attack can be severe. Therefore, preventing or at least quickly countering DDoS attacks can be critical for your organisation's survival.

Regularly testing your IT infrastructure is paramount to keeping your systems secure, and is something any organisation should consider as part of its cyber security strategy.

4. Computer viruses

What is a computer virus?

A computer virus is a type of malicious code or program written to alter the way a computer operates. Much like a flu virus, it is designed to spread from one computer to another (but without the user's knowledge) by:

- Opening an infected email attachment;
- Clicking an infected executable file;
- Visiting an infected website;
- Viewing an infected website advertisement; or
- Plugging in infected removable storage devices (e.g. USBs).

5. Attack vectors

Attack vectors are used to gain access to a computer or network in order to infect it with malware or harvest data.
There are four main types of attack vector:

DRIVE-BY
A drive-by cyber attack targets a user through their Internet browser, installing malware on their computer as soon as they visit an infected website.
It can also happen when a user visits a legitimate website that has been compromised by criminal hackers, either by infecting them directly or redirecting them to a malicious site.

ZERO-DAY ATTACK
Outdated (unpatched) software often contains vulnerabilities that criminal hackers can use to bring entire systems down. Where they exploit a vulnerability made public before a patch or solution has been rolled out by the developer, this is referred to as a zero-day attack.
Patch management is one of the five basic cyber security controls contained in the UK government's Cyber Essentials scheme.

MITM (man in the middle)
An MITM attack is where an attacker alters the communication between two users, impersonating both victims to manipulate them and gain access to their data. The users are not aware that they are communicating with an attacker rather than each other.

SQL INJECTION
A SQL (Structured Query Language) injection occurs when an attacker inserts malicious code into a server that uses SQL (a domain-specific language).
SQL injections are only successful when a security vulnerability exists in an application's software. Successful SQL attacks force a server to provide access to or modify data.

Protecting your organisation

Cyber attacks can cause significant disruption and damage to even the most resilient organisation. For those that fall victim, the reputational and financial repercussions can be devastating.

It is therefore important to have robust systems in place.

- Ensure that virus protection is update
- Ensure that web browsers are up to date
- Ensure that you take regular backups of date
- Take out cyber security insurance

What is your weakest link? Or is that who?

4/5 of the top causes of data breaches are because of human error
Information Commissioner’s Office (ICO), Data security incident trends, 2018

Educated and informed employees are your first line of defence. Empower them to make better security decisions with staff awareness training.

dte business advisers

- Business Advisory & Audit
- Tax Consultancy
- Corporate Finance
- Forensic Accounting
- Outsourcing & Payroll Management
- Financial Planning

THANK YOU!

DTE Business Advisers

DTE is a leading independent firm of chartered accountants and tax advisers in Bury, Manchester and North West England. We offer our accountancy services in Bury, Bolton, Rochdale and the rest of the North West.

Offering a range of services including auditing, accounting and tax advice to a diverse range of clients, we are a forward-thinking company who can help you realise the full potential of your business.

With 2 offices situated in the heart of Bury and Manchester, we have over 80 years' experience aiding a variety of businesses. Our expertise extends to working with owner-managed businesses, small to medium sized companies, business start-ups, and UK subsidiaries of large international groups.

All of our advisers are commercially minded and can help you to effectively work towards your long term goals.

At DTE Group, we believe you should only leave your finances in the hands of the best. Contact our accountants and tax consultants in Manchester to ensure your business is being well looked after.

FIND US IN BURY

The Exchange,
5 Bank street, Bury, BL9 0DN
Tel: 0161 767 1200 **Fax:** 0161 767 1201

Lower Bank St
Pizza Pioneer
Back Broad St
Silver St
Broad St
Castle Leisure Centre Car Park
Bolton Street Station Car Park
The Fusilier Museum
Library Gardens
Bury Art Museum
Kay G
The Art Picture House

FIND US IN MANCHESTER

6th Floor, Royal Exchange Building
St Ann's Square, Manchester, M2 7FE
Tel: 0161 819 1910 Fax: 0161 819 4749

Bodycare
ZARA
New Cathedral St
The Watch Lab
Manches
Three
schuh
Deansgate
Paperchase
ater
Royal Exchange Theatre
Market
HSBC Bank
St. Annes Square
Tesco Metro
aucho
Slater Menswear

dte business advisers

Our Services

- Tax Consultancy
- Forensic Accounting
- Business Advisory & Audit
- Corporate Finance
- IT Support
- Financial Planning
- Payroll Outsourcing

NEVER WORKED WITH DTE BEFORE?

*Book an initial **FREE**, no obligation consultation to see how we can help*

✉ marketing@dtegroup.com