Digital Deep Dive

Who am I?

owen@code56.co.uk

 @code_56

 /in/owen-conti

Golden Rules

- Engage experts early
- Delegate; Don’t abdicate
- Prioritise together
- Technology is a force multiplier
- Change is always happening
- Continuous improvement is business critical

Tools: Good, bad, and ugly

- Computers are everywhere
- Smart Phones
- Tablets
- TVs
- Cars (Apple Car Play, Android Auto)
- Watches
- Mouthguards!


ARCTIC OCEAN
Greenland
(Denmark)
Svalbard
(Norway)
ARCTIC OCEAN
United States
Canada
United States
Iceland
Norway
Sweden
Finland
Russia
U.K.
Den.
Neth.
Belg.
Ireland
Estonia
Latvia
Lithuania
Ger-
many
Poland
Belar.
Ukraine
Mol.
Kazakhstan
Mongolia
ATLANTIC
OCEAN
Portugal
Spain
France
Rom.
Bul.
Armenia
Geor.
Az.
Uzbek.
Turkm.
Kyrgyzstan
Tajikistan
China
Japan
N. Korea
S. Korea
Italy
Turkey
Cyprus
Greece
Syr.
Lebanon
Iraq
Iran
Afghan.
Pakistan
Kuwait
Qatar
Nepal
Bhutan
India
Laos
Vietnam
Taiwan
Bur.
Bangl.
Thai.
Cambodia
Philippines
Morocco
Tunisia
Algeria
Libya
Egypt
Israel
Jordan
Saudi
Arabia
U.A.E.
Oman
Yemen
Djibouti
Western
Sahara
Mexico
Caribbean
Maurit.
Mali
Niger
Chad
Eritrea
Sudan
Senegal
The Gambia
Guinea-Bissau
Guinea
Sierra Leone
Liberia
Cote d'Ivoire
B.Faso
Ghana
Togo
Benin
Nigeria
Cam.
C.A.R.
South
Sudan
Ethiopia
Somalia
Ken.
Uganda
Rwanda
Burundi
Tanz.
Sri
Lanka
Malaysia
Indonesia
Timor-Leste
Papua
New Guinea
Solomon
Islands
PACIFIC
OCEAN
Central
America
Guyana
Suriname
French
Guiana
(France)
Venez.
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
Equatorial Guinea
Gabon
Congo
Dem.
Rep. of
Congo
Angola
Zambia
Zim.
Bots.
Namibia
South
Africa
Lesotho
eSwatini
Mozambique
Malawi
Madagascar
INDIAN
OCEAN
ATLANTIC
OCEAN
Australia
New
Caledonia
Fiji
New Zealand


HOTEL
PHOTOGRAPHY
GENERAL STORE
BILLIARDS

How does IT change at scale?

- Micro (<10 people)
- Small (10 – 49 people)
  - Around 15 people
  - Around 30 people
- Medium (50 – 249 people)
  - Over 50 people
  - Over 150 people
- Large (>250 people)

First Steps:
Cyber Essentials

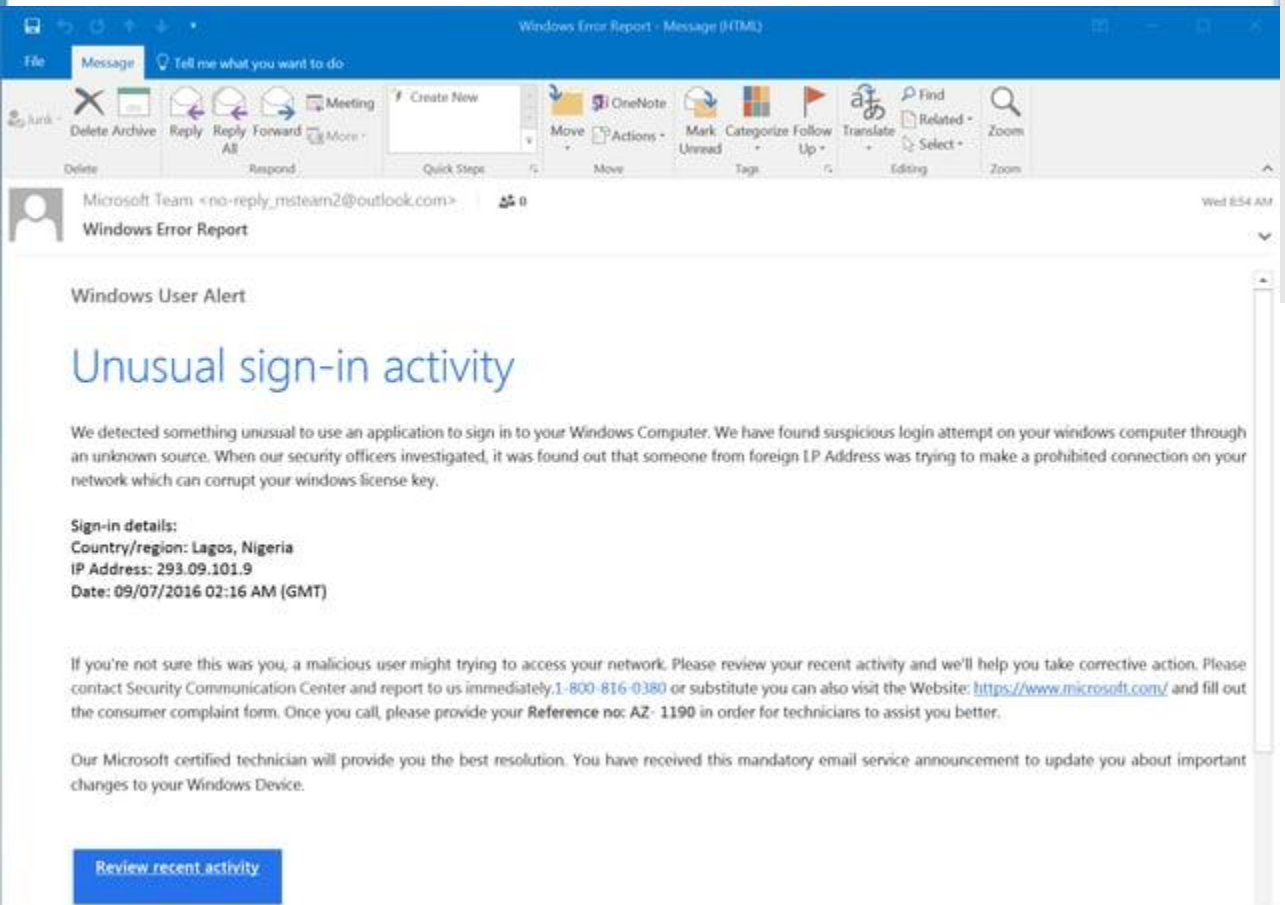
What would happen if you never updated again?

How to spot an attack

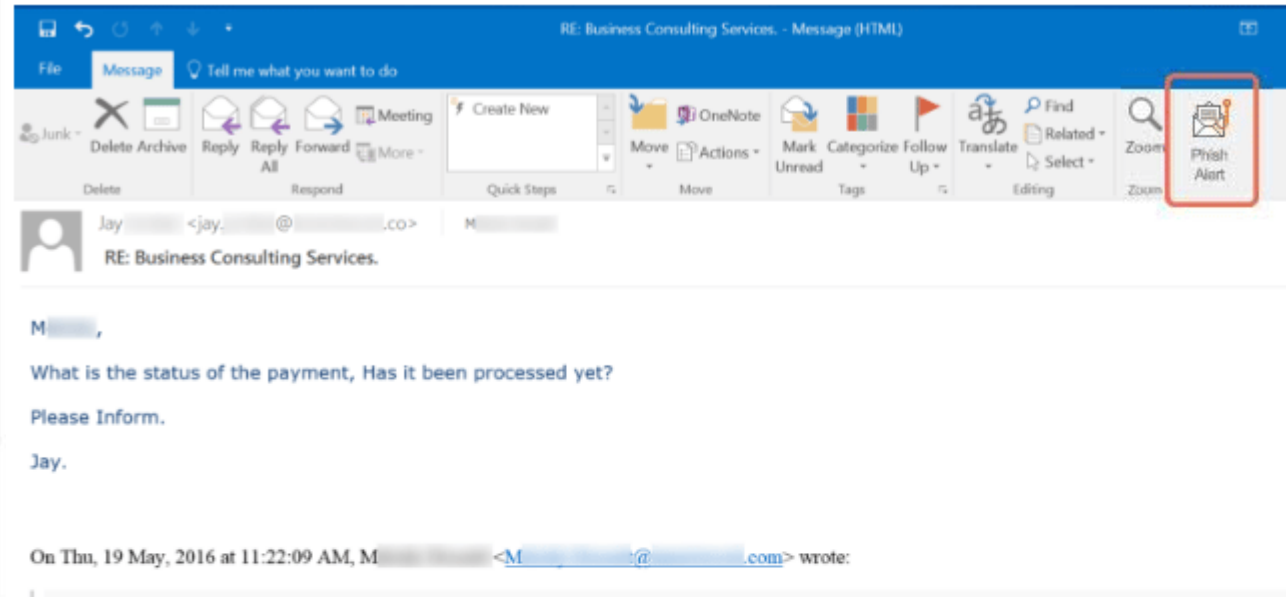
Phishing

Ransomware


Adobe ID
Sign in with your email and password
Adobe
Receiver Email address
Stay signed in
This PDF is protected
Uncheck on public devices.
VIEW FILE


Windows Error Report - Message (HTML)
Microsoft Team <no-reply_msteam2@outlook.com>
Windows Error Report
Windows User Alert
Unusual sign-in activity
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.
Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to assist you better.
Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.
Review recent activity


confirmation_2321821.doc [Compatibility Mode] - Word
Enable Content
Microsoft Office
This document is protected.
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.


RE: Business Consulting Services. - Message (HTML)
RE: Business Consulting Services.
What is the status of the payment, Has it been processed yet?
Please Inform.
Jay.
On Thu, 19 May, 2016 at 11:22:09 AM, M

How to spot an attack

Phishing

Ransomware

YOUR COMPUTER HAS BEEN LOCK

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

[redacted]

OK

NoCry Decryptor

Ooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

Your files will be lost on :

71 : 58

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin

Send $100 worth of bitcoin to this address:

1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

Copy

Show Encrypted Files

Decrypt

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

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

raised on

lost on

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

How to react

1. Acknowledge you're about to have a Bad Day®
2. Pull out your "Oh <expletive of choice>" file
3. Be systematic, calm, and try to process the emotions in a productive manner


Story Time

Consequences

- Unplanned Outage
- Customer service & delivery issues
- Reporting to ICO
- Reputational damage
- Customer trust damage
- Costs
  - Lost opportunities
  - Distraction
  - Unplanned IT equipment
  - Lost productivity

Investment

(Sorry, there’s no magic formula)

Help Desk	Web Design	Disaster Recovery
Application Management	Software Development	Data Protection
Management Information Systems	IT Infrastructure	Asset Management
Information Security	Database Management	CCTV & Access Control
Risk Management	Software Testing	Printers
Telecoms & Unified Communications	Automation	Network Management & Connectivity
Project Management	Process Design & Review	Lifecycle Management

IT is about:

Enabling productivity

Ensuring security

Protecting Business continuity

Enabling productivity

- Check your IT subscriptions
  - Upgrades & new apps?
  - Double paying somewhere?
- Are there any repetitive processes/procedures that could be automated?
- Is the set up still suitable for how things are done today?
- Can Template files be used (instead of copy & save as)?

Ensuring security

- Review how you manage shared passwords
- Use a Password Manager
- Use Multifactor Authentication (MFA / 2FA)
- Check out Cyber Essentials
  - Updates & patches
  - Least privilege
  - Perimeter security
  - Modern antivirus

Protecting Business continuity

- 3-2-1 Backup
  - 3 copies
    - (Working, Backup, + Offsite Backup)
  - 2 different media
  - 1 off-site
- Do a test restore on a routine schedule
- Write an “oh <insert favourite swear word>” bullet point list
  - A.k.a. a “Disaster Recovery Plan”

owen@code56.co.uk

@code_56

/in/owen-conti


56

Blankety Blank

1. MFA stands for multi BLANK authentication. (Factor)
2. A BLANK attack is when someone is tricked into entering their username and password on a fake website. (Phishing)
3. Malware is a portmanteau of BLANK and software. (Malicious)
4. John Edwards is the current head of the Information BLANK Office in the UK. (Commissioners)
5. Later this month Microsoft Windows turns BLANK years old. (37)
6. A BLANK is used to secure the perimeter of a network. (Firewall)
7. An ethical hacker is also sometimes known as a BLANK hat hacker. (White)
8. Attackers use programmes that try password after password in BLANK force attacks. (Brute)
9. A good password should be at least BLANK characters long. (12)
10. Botnet is a portmanteau of robot and BLANK. (Network)
11. It's very important to apply BLANKS in a timely manner to keep your systems secure. (Updates)
12. If you get hit by ransomware the only way out of it is to restore from BLANK. (Backups)
13. It is widely thought that an attacker has normally had access to a system for BLANK days before they execute their main attack. (279)
14. It is possible to rent ransomware-as-a-service on the BLANK web. (Dark)
15. Edward Snowden used to work for the BLANK in America. (NSA)
16. If you experience a data breech you may need to disclose it to the BLANK. (ICO)
17. You should BLANK pay the ransom if you get hit by ransomware. (Never)
18. DDOS stands for BLANK denial of service, and uses a botnet to launch an attack. (Distributed)
19. The Cyber Essentials Readiness tool costs BLANK to download. (Nothing)
20. Like Onions, and Ogres, the best Cyber Security has BLANKS. (Layers)