Webinar: Key Security Measures for NFPs Implementing Remote Work

21st April 2020

Thank you for joining – we’ll be starting soon

Please note this webinar may be recorded.

the I.T. team™

Maintaining the health of your I.T. system

WHAT WE WILL COVER TODAY?

- Importance of Security
- Overview of the variety of threats
- Real-life examples of breach attempts
- Remote working and its impact on Security
- Protection measures you need to take and how to get started
- The training options for your team

About the I.T. team

- Formed in 2011
- Office 365 since its inception
- Managed Services/IT support
- A wide range of IT services
- Major NFP base of customers
- Providing IT services to NZ & Australian organisations

the I.T. team™
Maintaining the health of your I.T. system

SECURITY FACTS

- $600 billion, or nearly 1% of global GDP, is lost to cybercrime every year
- Global ransomware damage costs are expected to exceed $11.5 billion annually by 2019
- 30% of organizations experienced a successful ransomware attack over the past year
- 27% of organizations encountered a CEO fraud attack in the past 12 months
- Microsoft detect 200 million phishing emails every month
- Average age of a typical Cybercriminal is 17.

MAJOR BREACHES

- Carbanak phishing attack - $1.2 billion
- Yahoo - 3 billion records
- Adult Friend Finder – 412 million records
- eBay - 145 million records
- Equifax – 143 million records
- Ashley Madison - 60 gigabytes of company data

WHY SECURITY IS IMPORTANT

- Data is valuable
- Consequence of Breach:
  - Productivity Impact
  - Financial Impact
  - Reputation Impact
- One Breach will likely lead to a further breach
- Low Impact breaches tend to create the opportunity for a higher impact breach (often by other parties).

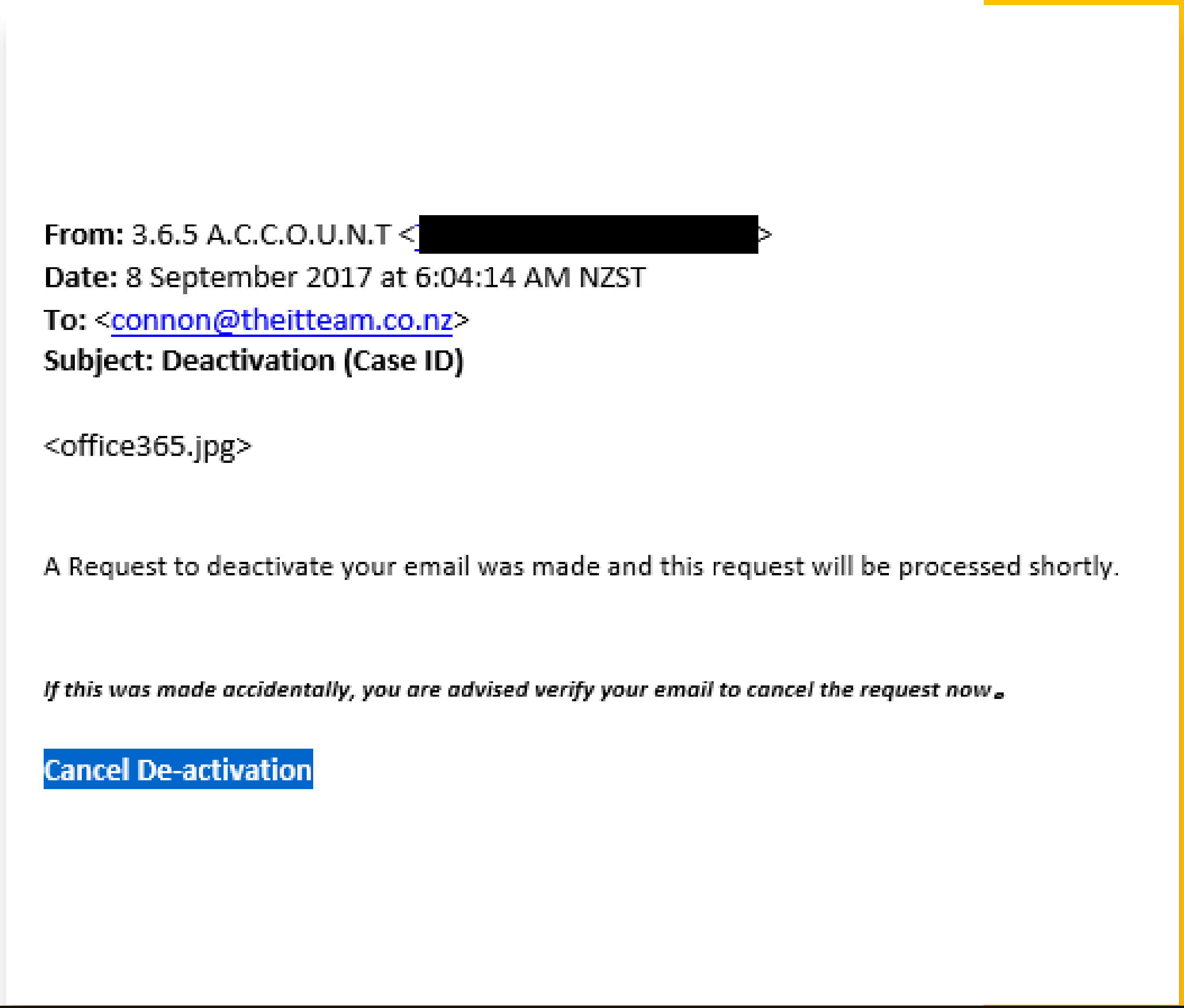
COMMON THREATS

PHISHING

Sending emails imitating reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers

Generally the most common and popular type of security threat out there and the most likely to succeed.

PHISHING EXAMPLE: Deactivation Scare



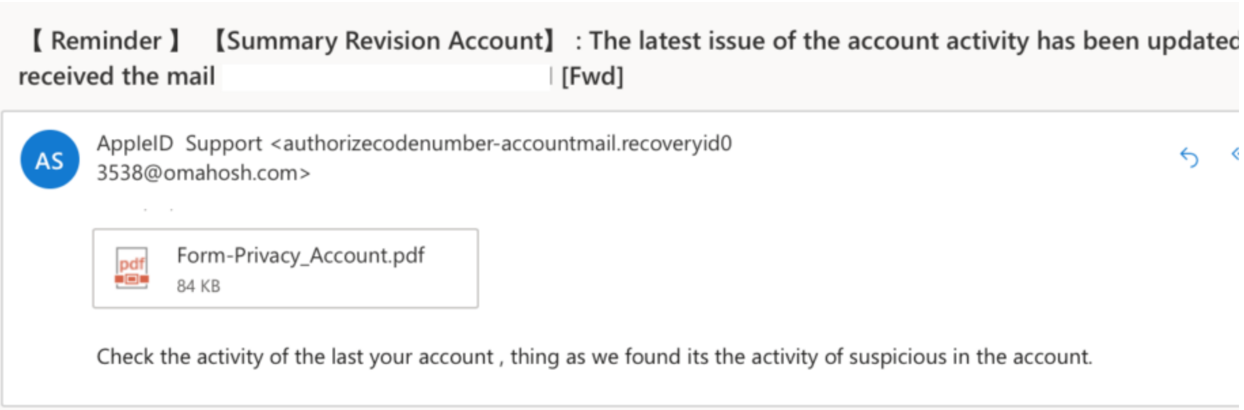
From: 3.6.5 A.C.C.O.U.N.T <[redacted]>
Date: 8 September 2017 at 6:04:14 AM NZST
To: <connon@theitteam.co.nz>
Subject: Deactivation (Case ID)

<office365.jpg>

A Request to deactivate your email was made and this request will be processed shortly.

***If this was made accidentally, you are advised verify your email to cancel the request now*.**

PHISHING EXAMPLE: PDF Attachment Scam



【 Reminder 】 【Summary Revision Account】 : The latest issue of the account activity has been updated received the mail [redacted] [Fwd]

AppleID Support <authorizecodenumber-accountmail.recoveryid03538@omahosh.com>

Form-Privacy_Account.pdf
84 KB

Check the activity of the last your account , thing as we found its the activity of suspicious in the account.

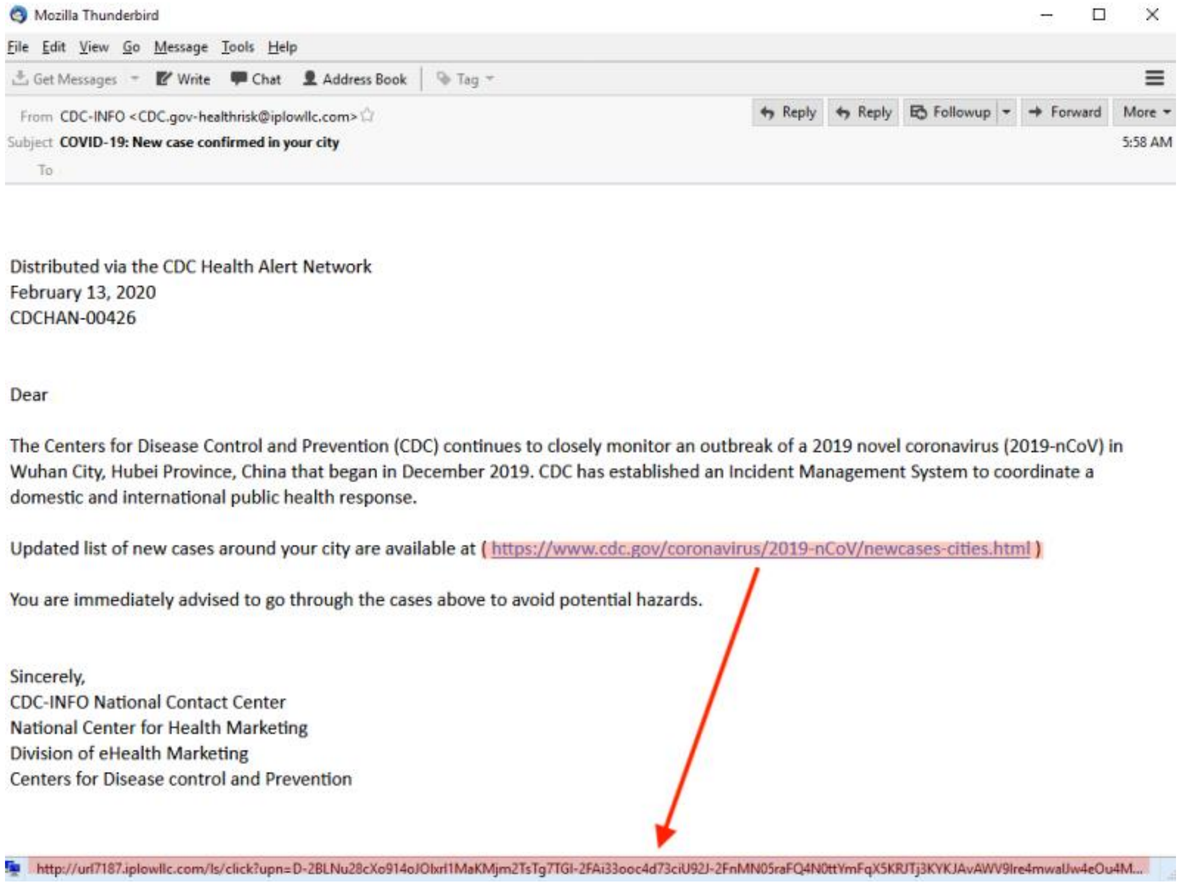
COVID19 PHISHING

- Users targeted by coronavirus-themed phishing emails, with infected attachments containing fictitious 'safety measures’.
- Instead of the link containing health information, it instead installs malicious software on your device that’s designed to steal personal information.
- Similar emails being circulated that encourage people to fill in their email and password before they can get information on COVID-19.

PHISHING – COVID19

- Some people are receiving emails claiming to be from the World Health Organisation (WHO).
- These emails have COVID-19 in the subject line, and request the recipient **donate** to the WHO COVID-19 Response Fund
- These mails are not from the WHO, and any money donated will go to the scammers.

PHISHING EXAMPLE: FAKE LINK



From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>

Subject **COVID-19: New case confirmed in your city**

5:58 AM

To

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

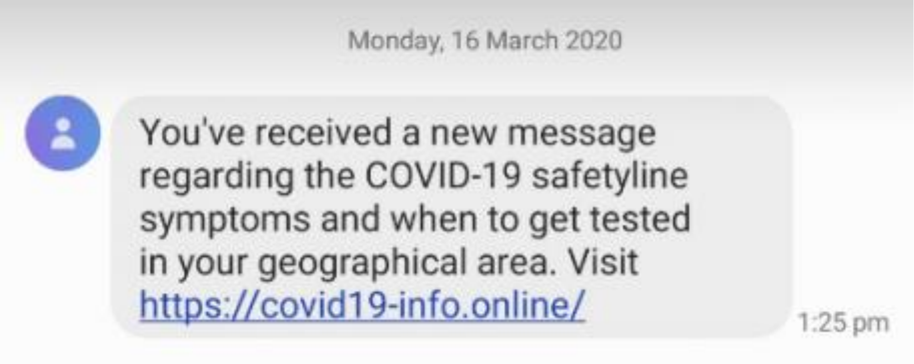
You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

http://url7187.iplowllc.com/ls/click?upn=D-2BLNu28cXo914oJOlxrl1MaKMjm2TsTg7TGI-2FAi33ooc4d73ciU92J-2FnMN05raFQ4N0ttYmFqX5KRJTj3KYKJAvAWV9lre4mwalJw4eOu4M...

TEXT MESSAGE SCAMS

- Reports have been received in Australia of COVID-19 themed scam text messages
- This link is not legitimate & may install malicious software designed to steal personal info and/or banking details.



Monday, 16 March 2020

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

1:25 pm

FAKE CORONAVIRUS MAPS

- Attackers claim to have a ‘coronavirus map’ application that people can download onto their devices
- Instead, the application is malware, designed to steal sensitive information from the device it is downloaded onto, such as passwords

PHISHING: POTENTIAL FIXES

- User Education
- Multi Factor Authentication
- Mail Filtering systems
- DNS filtering (i.e. Cisco Umbrella)

SPEAR PHISHING (AND WHALING)

Definition

*the fraudulent practice of sending emails ostensibly from **a known or trusted sender** in order to induce targeted individuals to reveal confidential information.*

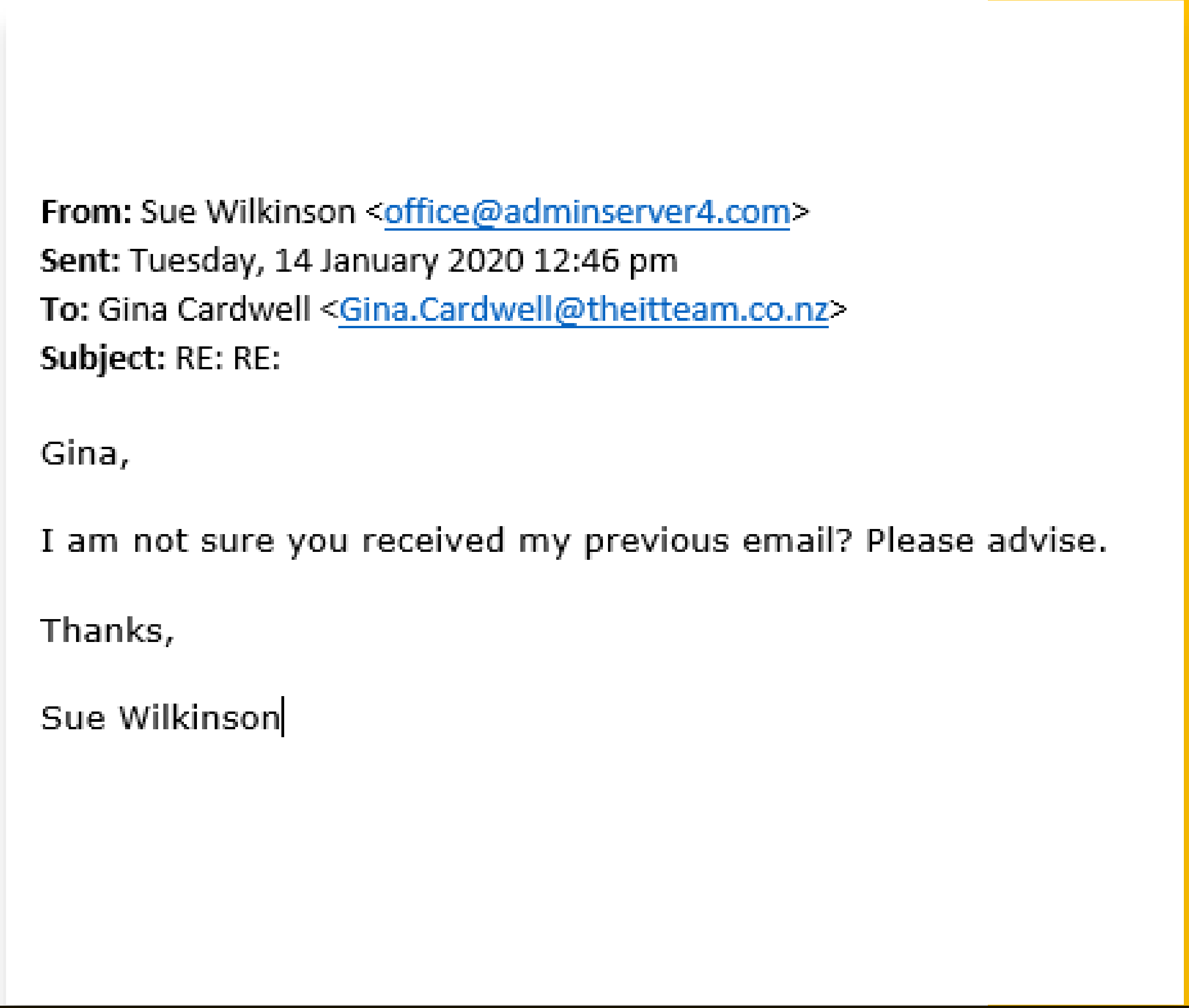
SPEAR PHISHING

- Spear phishing and whaling are email scams, but they're much harder to spot than phishing
- The emails look like they’ve come from someone within the company, so you’re much more likely to trust them
- The attacker's aim is to get information about your organisation, for example:

  a. staff credentials
  b. financial information
  c. personally identifiable information (PII) about your customers
  d. trade secrets or intellectual property (IP).

- Sometimes used as a follow on from a successful phishing attempt

SIMPLE SPEAR PHISHING EXAMPLE



From: Sue Wilkinson <office@adminserver4.com>
Sent: Tuesday, 14 January 2020 12:46 pm
To: Gina Cardwell <Gina.Cardwell@theitteam.co.nz>
Subject: RE: RE:

Gina,

I am not sure you received my previous email? Please advise.

Thanks,

Sue Wilkinson

CASE STUDY – SIMPLE CEO FRAUD

From: John Smith
Sent: Monday, 13 November 2017 11:27 AM
To: Susan Brown

Subject: Urgent Attention

Are you available to handle an international payment this morning? Have one pending, let me know when to send bank details.

Regards
John Smith

Sent from my iPhone

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 1:33 PM, Susan Brown wrote:

Hi John,

Sorry was caught up with a project – I'm here now – can I still help?

Susan Brown
Office Admin

CASE STUDY - SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 4:29 PM, John Smith wrote:

Can you still handle this right now? was very busy earlier.
Regards

John Smith

Sent from my iPhone

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 6:01 PM, Susan Brown wrote:

Hi John,

Just back – can do it for you now if that will help.

Cheers,
Susan Brown
Office Admin

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 6:48 PM, John Smith wrote:

Yes it seem to be a very busy day. The amount is for $62,120 i am guessing it is very late already for the transfer or can you still get it done today?

Regards
John Smith

Sent from my iPhone

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 6:58 PM, Susan Brown wrote:

Hi John,

Is it set up ready to go in PC banking?
I can’t see it there to authorise under international?

Cheers,
Susan Brown
Office Admin

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 7:05 PM, John Smith wrote:

Oh ok, please find a way around it, my day is really tied. Can I send you the bank details today still? Can the payment still go out?

Regards
John Smith

Sent from my iPhone

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 6:58 AM, Susan Brown wrote:

Hi John,
I can do my best but will do it from home tonight as have to leave the office now. Think they still go to 8 pm or so.
Send me all the details and I'll try but usually Mary sets them up and we just authorise them.
Will see what I can do – it's no trouble as I know I can ask Mary from home if necessary.

Leave it with us.

Regards,
Susan Brown
Office Admin

CASE STUDY – SIMPLE CEO FRAUD

On Mon, Nov 13, 2017 at 7:02 AM, John Smith wrote:

Ok then. Thanks
NAME: Acme
SORT CODE: 12341234
ACCOUNT: 123412341234
IBAN: ABCD12341234123412341234
SWIFT ABC:ABCD1234
BANK: SOME BANK
ADDRESS: 3 Somewhere Place
Send me payment slip once it is completed.

Regards

John Smith
Sent from my iPhone

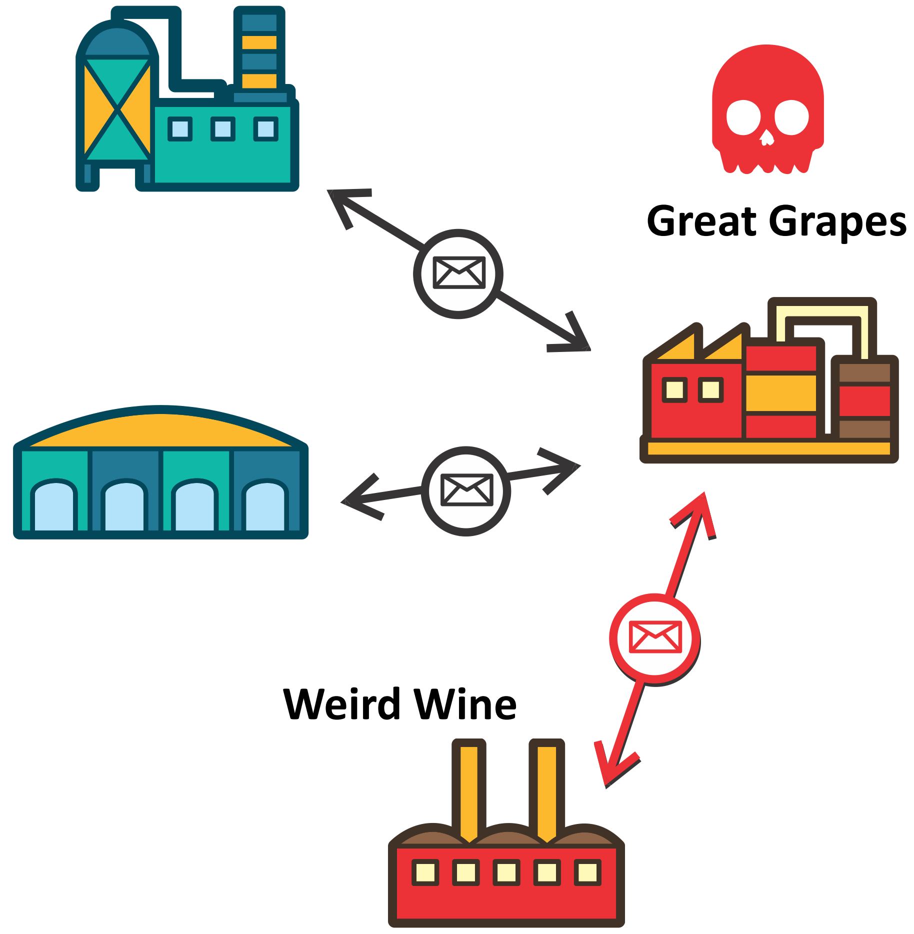
CASE STUDY – SIMPLE CEO FRAUD

KEY POINTS

- Simple view of email address would have revealed the fraud
- Poor use of language
- Sense of urgency
- Procedure was changed
- No second channel of verification
- “No question” culture

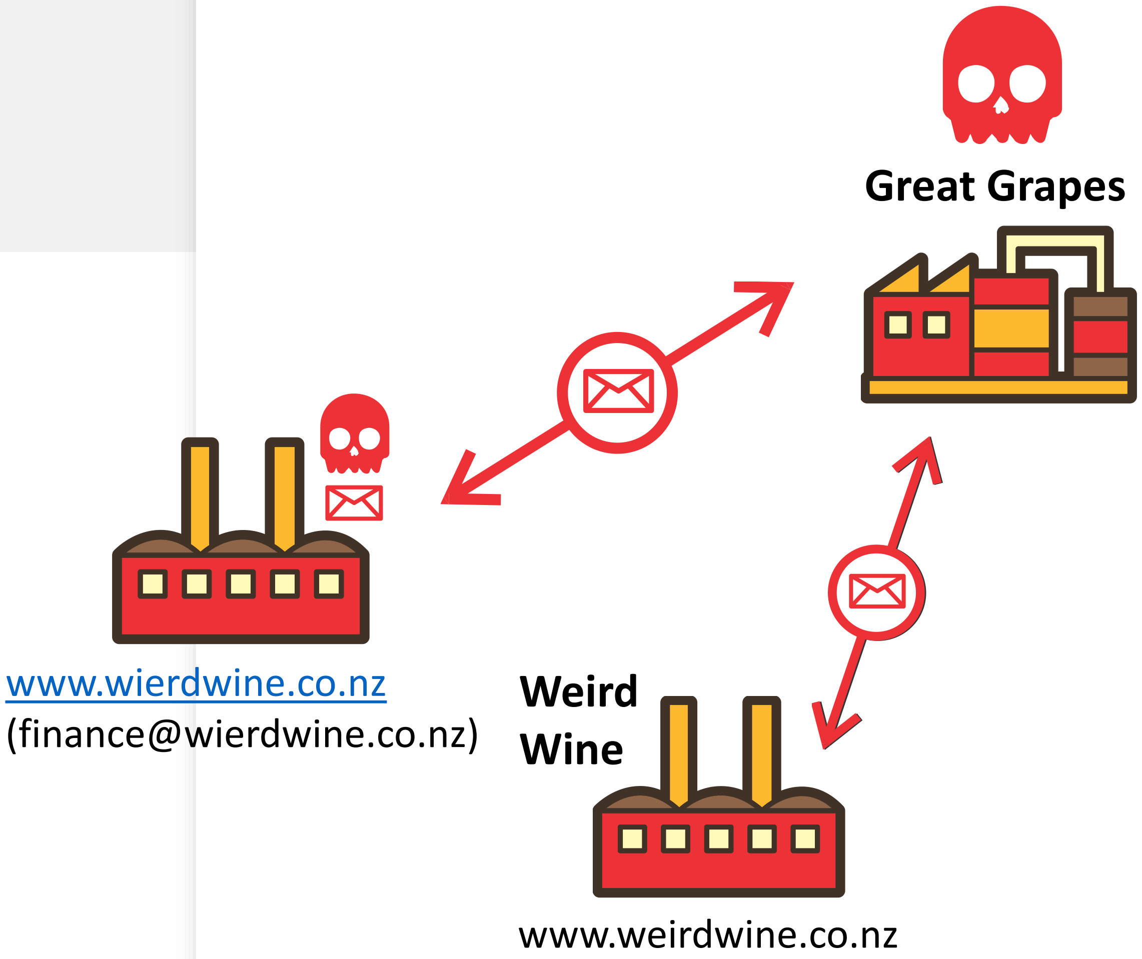
CASE STUDY – LONG GAME SPEAR PHISHING EXAMPLE

- Hacker hacks Great Greats (contractor to Weird Wine) – Office 365 via phishing attempt.
- Had access to all emails.
- Lies dormant for several months reviewing behaviours
- Hacker registers domain with minor spelling error – wierdwine.co.nz instead of weirdwine.co.nz



CASE STUDY - COMPLEX SPEAR PHISHING EXAMPLE

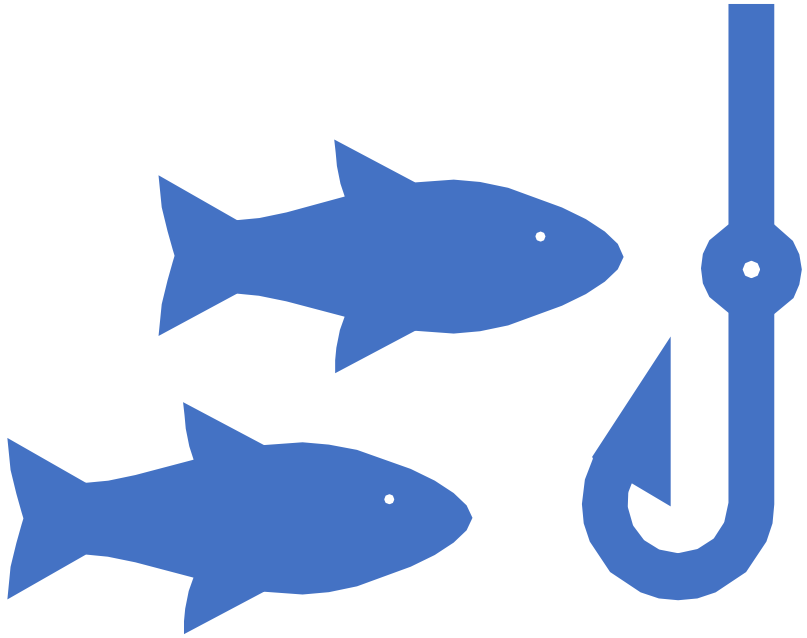
- Hacker changes email rules so legitimate emails from WC to GA are diverted to deleted items.
- Hacker then sends an email from GA to WC instructing alternate payment details.
- WC pay the GA invoice but it goes to the Hackers account.



CASE STUDY - COMPLEX SPEAR PHISHING EXAMPLE

KEY POINTS

- Smart thinking from the hacker. Registered similar domain.
- Patience - Reviewed payment behaviour for several months
- Procedure was changed
- No second channel of verification for bank details



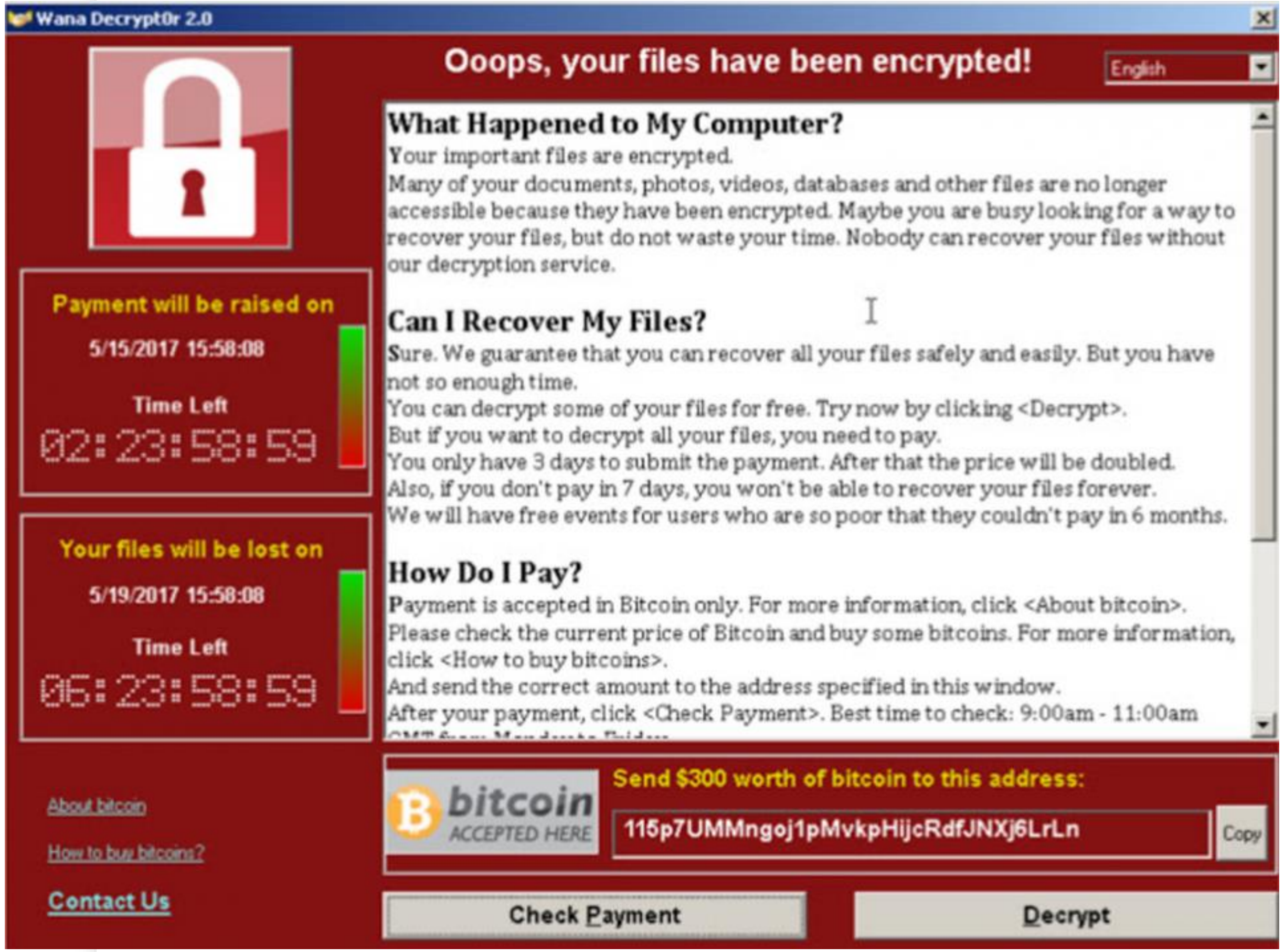
SPEAR PHISHING: POTENTIAL FIXES

- DMARC (with DKIM & SFP)
- Mail Filtering systems
- User education

RANSOMWARE

Definition

- "a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid."



Ooops, your files have been encrypted!

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:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

CASE STUDY RANSOMWARE

RECOVERY EFFORT

- Restore from cloud backups – 36 hours downtime.
- Bespoke application-specific data was restored from a decommissioned server (lucky!).
- Productivity was crippled for this period.

MITIGATION

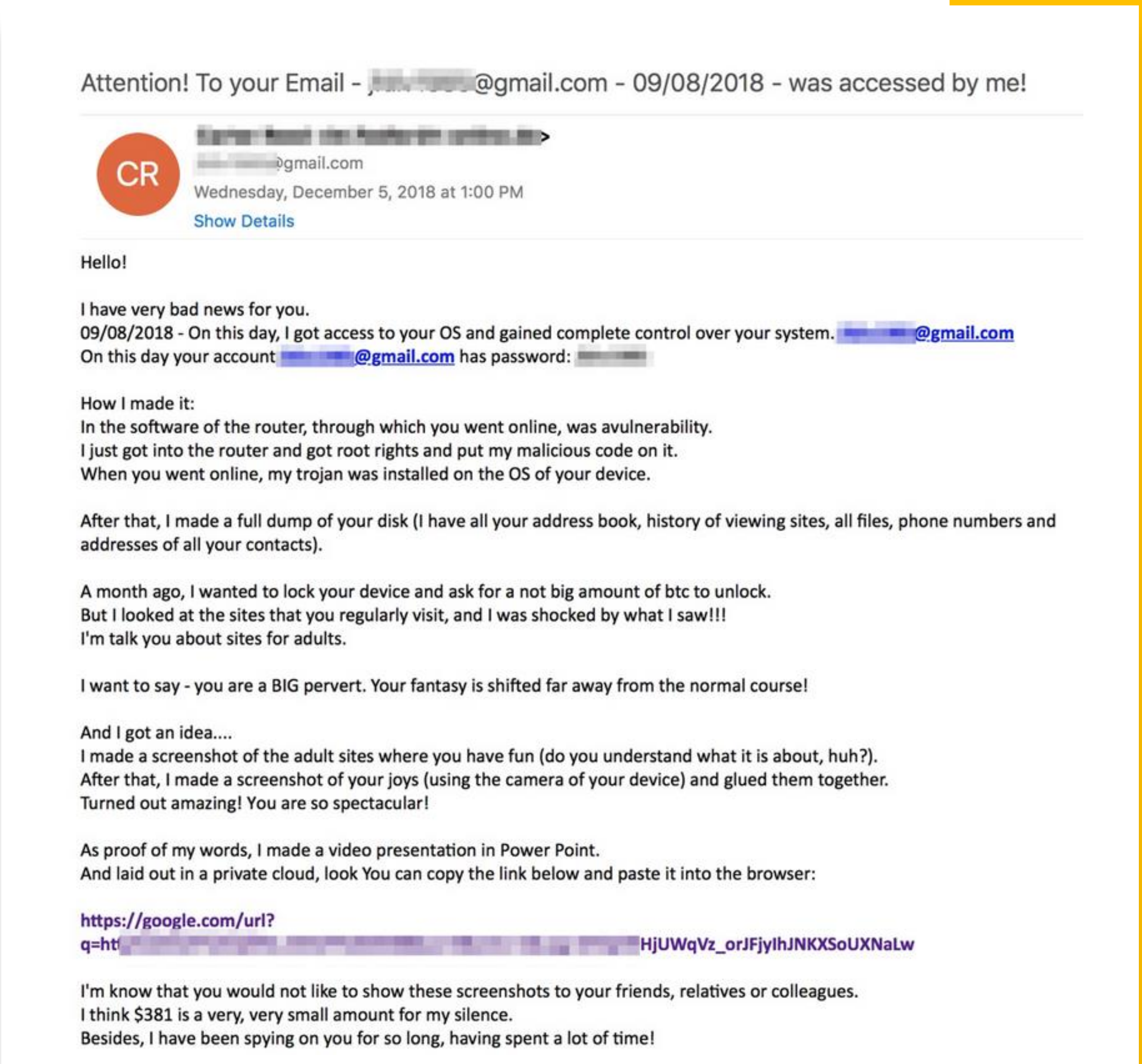
- Implement secured access to RDP sessions via a secure tunnel in the form of a VPN connection
- Only allow secured machines to access resources on the company network. If users need to work from home, use machines protected and managed by the company mandated security systems.
- Restrict users permissions/access

PHONECALL SOCIAL ENGINEERING

- Generally phone-based requests to gain access.
- Threat of virus or infection to access machine.
- Impersonates Microsoft, Intel etc.
- Frequently from India
- Tech support accesses computer, makes it appear there is breach. Requests passwords, credit cards. Cleans out and fixes.

WEBCAM EXTORTION SCAMS

- Scam emails are asking recipients to pay money to the sender or they will circulate video footage of the recipient in compromising positions
- Send a copy of a legit password that has been found on the Dark Web
- This is a common scam, but newer variations are threatening to spread coronavirus to their family if they don't pay the ransom.



Attention! To your Email - [redacted]@gmail.com - 09/08/2018 - was accessed by me!

CR [redacted]>
[redacted]@gmail.com
Wednesday, December 5, 2018 at 1:00 PM
Show Details

Hello!

I have very bad news for you.
09/08/2018 - On this day, I got access to your OS and gained complete control over your system. [redacted]@gmail.com
On this day your account [redacted]@gmail.com has password: [redacted]

How I made it:
In the software of the router, through which you went online, was avulnerability.
I just got into the router and got root rights and put my malicious code on it.
When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.
Turned out amazing! You are so spectacular!

As proof of my words, I made a video presentation in Power Point.
And laid out in a private cloud, look You can copy the link below and paste it into the browser:

https://google.com/url?
q=ht[redacted]HjUWqVz_orJFjylhJNKXSoUXNaLw

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.
I think $381 is a very, very small amount for my silence.
Besides, I have been spying on you for so long, having spent a lot of time!

3RD PARTY SITE Credential Breach

- Linkedin
- MySpace
- Tumblr
- Adobe
- MyFitnessPal
- Many, many others

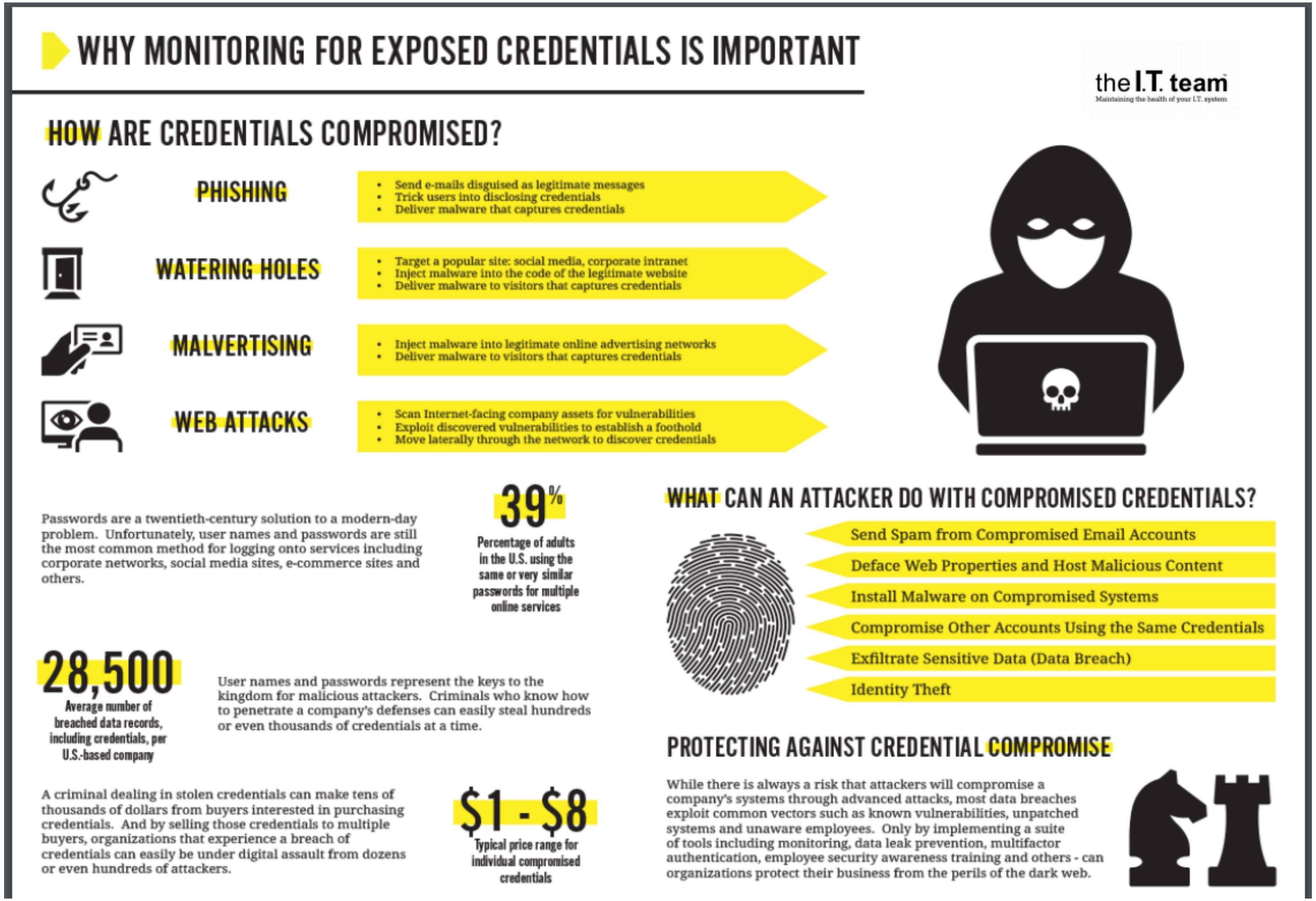
haveibeenpwned.com

3RD PARTY SITE Credential Breach - Remedies?

POTENTIAL PROTECTIONS AND REMEDIES

- Dark Web Monitoring
- Avoid password reuse, Reset passwords that are similar.
- Make changes to Password Manager setup/passwords
- Multi Factor Authentication

DARK WEB



WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

the I.T. team™
Maintaining the health of your I.T. system

HOW ARE CREDENTIALS COMPROMISED?

PHISHING
- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

WATERING HOLES
- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

MALVERTISING
- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

WEB ATTACKS
- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

39%
Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500
Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

$1 - $8
Typical price range for individual compromised credentials

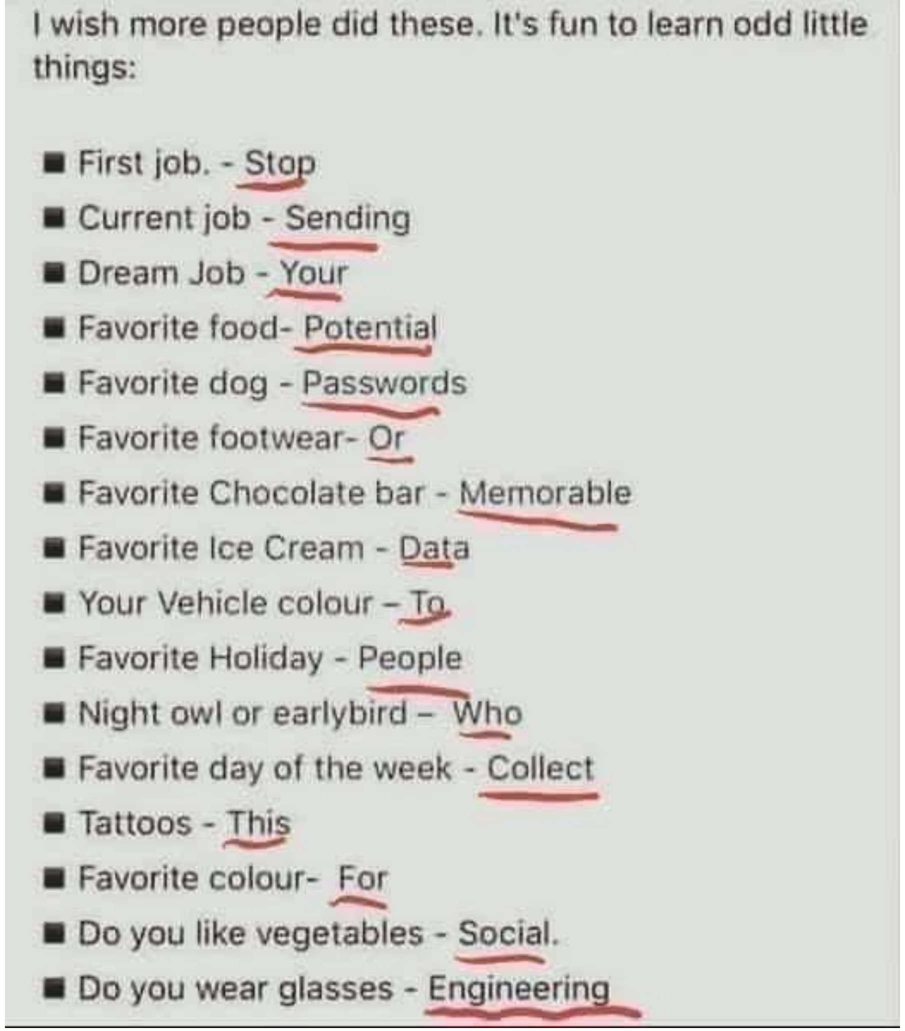
WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?

- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.

PRIVACY -DATA HARVESTING



I wish more people did these. It's fun to learn odd little things:

- First job. - Stop
- Current job - Sending
- Dream Job - Your
- Favorite food- Potential
- Favorite dog - Passwords
- Favorite footwear- Or
- Favorite Chocolate bar - Memorable
- Favorite Ice Cream - Data
- Your Vehicle colour – To
- Favorite Holiday - People
- Night owl or earlybird – Who
- Favorite day of the week - Collect
- Tattoos - This
- Favorite colour- For
- Do you like vegetables - Social.
- Do you wear glasses - Engineering

REMOTE WORKING

WHAT HAS CHANGED?

REMOTE WORKING

- Personal Workstations (shared with others)
- VPN's (esp. with Shared Workstations)
- Firewall and basic security settings on home machines
- Workstations not on your Domain
- Lack of MFA (due to rapid deployment)
- Personal devices accessing company networks and data

REMOTE WORKING

- Targeted Phishing Attempts related to Remote Working
- More isolation for people to fall victim (more in further slides)
- Services like Zoom are particularly vulnerable to Phishing at present

REMOTE WORKING

- Is sensitive data being stored where it shouldn’t be?
- Storing business docs on Personal Workstations (also could have Backup issues)
- Rapidly setup Teams/Sharepoint/DropBox instances with Permissions issues

REMOTE WORKING ISOLATION

- Users are Isolated
- Harder to ask for help
- Natural chatter when something dodgy occurs is reduced
- More difficult to determine when users are struggling technically
- Approvals are more likely to be via email than before
- In an emergency situation lapses are understandable but at a certain point we need to bring standards back.

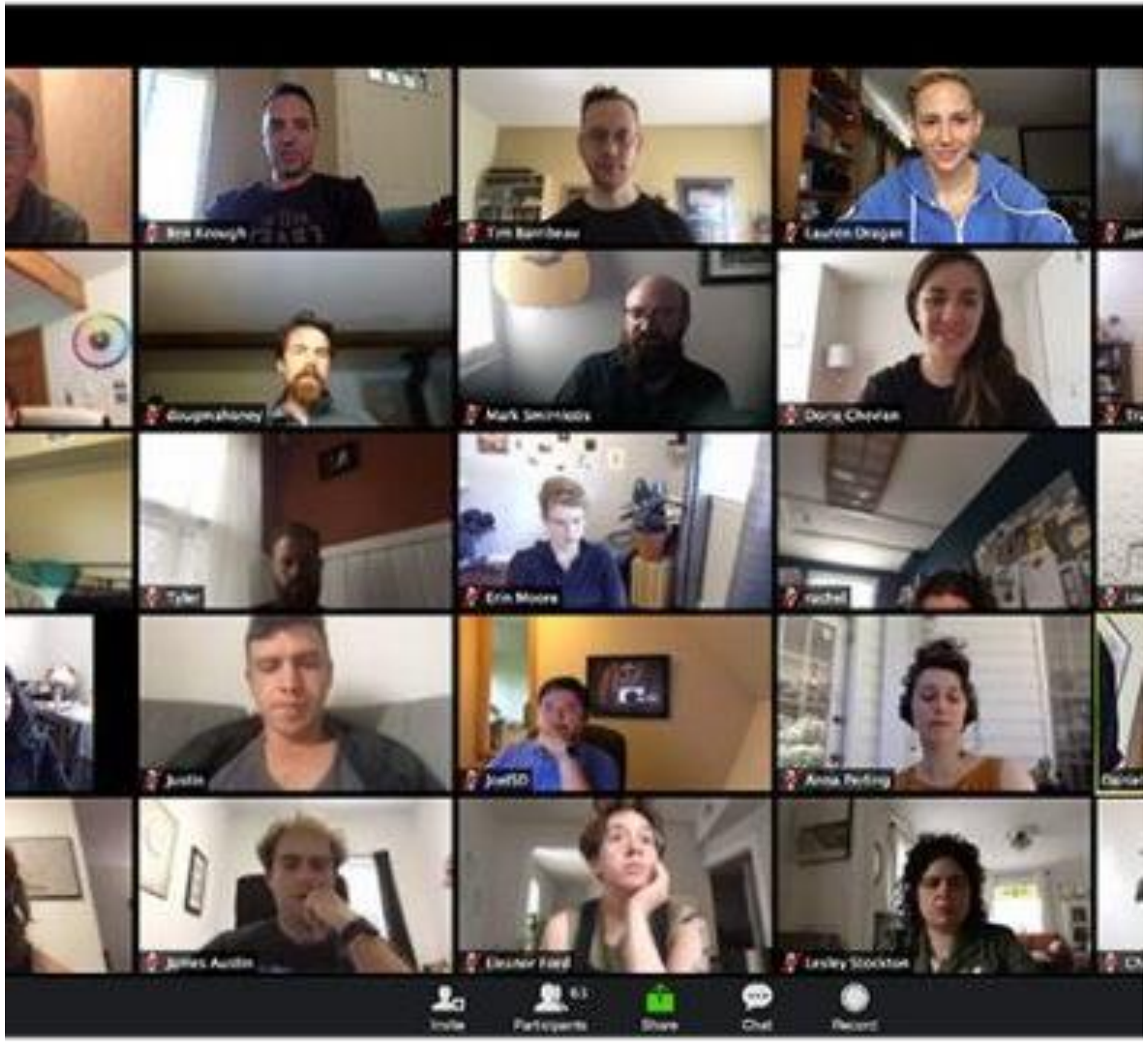
REMOTE WORKING – SECURITY QUICK WINS

- Ensure minimum protection on home workstations – Antivirus, Separate Accounts, Up to Date, Firewalls enabled.
- Get MFA operational on your email service and any other key services.
- Plan Permissions structure review (if new services exist).
- Consider your protection against Phishing, options exist.
- Consider policies for your organisations/staff (i.e. BYOD)
- Encourage check ins and verifications to occur even more than before
- Encourage sharing of experiences

VIDEO CALLING & CONFERENCING

- Zoom, Teams, Skype, Messenger Video, WhatsApp all broadly used
- Zoom the most popular, gone from 10 million daily users in December 2019, to 200 million in March 2020.

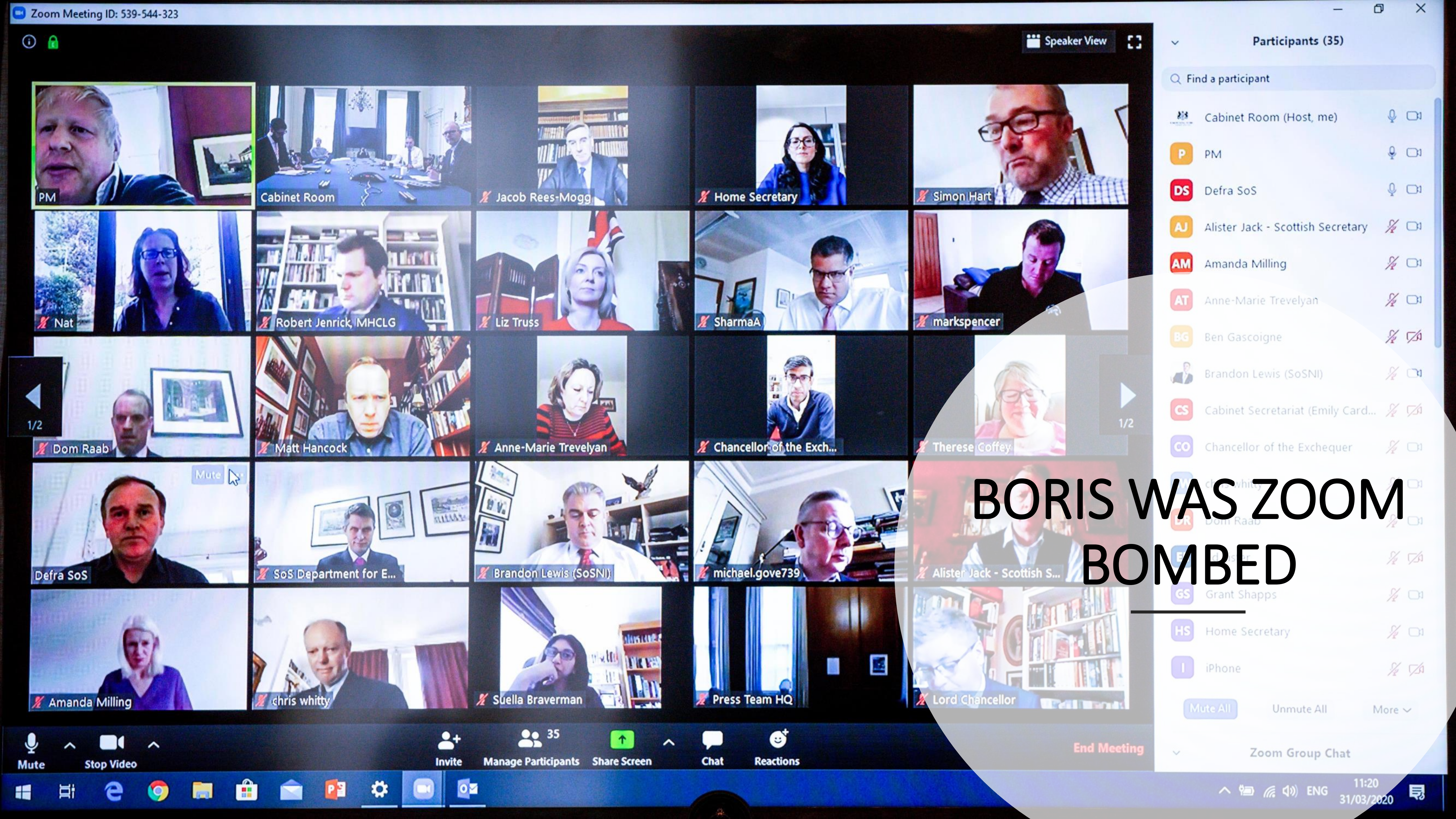
- Rapid uptake from users and organisations
- Easy to get started
- Little training given
- Struggling users more isolated
- Issues with tech and lack of understanding of security heightened



ZOOM BOMBING

- ***Zoom bombing*** is shorthand for when strangers intrude on others' meetings on Zoom.
- Sometimes, they might just listen in without anyone knowing they're there.
- Other times, they totally disrupt the meetings in silly or even threatening ways.

BORIS WAS ZOOM BOMBED



ZOOM BOMBING – WHAT HAVE THEY DONE?

- Changed its default settings so that every meeting is automatically assigned a required password to enter it
- A "waiting room" feature is now automatically enabled when you set up a meeting. This prevents users from joining a call before they've been screened by the host
- The meeting ID code is not shown in the title bar during a Zoom meeting.
- If you want to be super-secure you should change up your meeting ID with every call and password too.
- Moving rapidly to fix security and privacy issues in next 90 days, moratorium on feature enhancement until that is completed.

WHAT ABOUT MS TEAMS?

- 20 million daily active users (Nov) to 44 million (April)
- Security a cornerstone of the Office 365 suite.
- You can decide who from outside your organisation can join your meetings directly, and who should wait in the lobby for someone to let them in
- You can remove participants during a meeting
- Designate 'presenters' and 'attendees', and control which meeting participants can present content
- Teams doesn't use data to serve ads and it does not track participants' attention in meetings (Zoom has previously)
- Teams encrypts data in transit and at rest (SRTP)

PROTECTION MEASURES - DEVICE

Install software updates

- Keeping your devices and software up-to-date is one of the most effective things you can do to keep your system safe. You need to make sure:

Secure your devices

- Enable anti-malware software on any device that accesses your business data or systems. It prevents malicious software — such as viruses or ransomware — from being downloaded. This includes both company owned devices and any BYOD devices that belong to your staff. Malware's easier to avoid than it is to fix, and there are some simple things you can do to minimise your risk.

Back up your data

- If you run a business, you know how important it is to keep your data safe. If it's compromised in any way — if it's lost, leaked or stolen, for example — you need to make sure you have a backup, or copy, available so you can restore it.

PROTECTION MEASURES - NETWORK

Network

- With cloud systems being used so much these days, business networks are much smaller than before. Cloud systems are all internet based, but some organisations may still have a few servers hosting software that's only accessible from the office. Others may host their web applications in a cloud environment like Amazon Web Services (AWS).

Log Access

- when an incident may be about to occur — for example, when you've had multiple failed logons to your network, or
- when an incident has occurred — like a logon from an unknown IP address in Uzbekistan.

Update your default credentials

- Default credentials are login details that give the user administrator-level access to a product. They should only be used for the initial setup, and then changed afterwards.

PROTECTION MEASURES - USERS & POLICY

- No matter how well you prepare, sometimes things go wrong. Plan before to reduce stress at the time.

- Require notifications from staff – Included in company policy.
- Response Plan – Plan how to respond.
- Breach notification – Plan how to notify people affected.

PROTECTION MEASURES - TECHNOLOGY

- MFA
- DKIM/DMARC
- DNS Filtering
- 365 Backup
- Quarantine system in office 365
- Azure AD / Domain
- Office 365 Score

TRAINING

- Consider the wider team
- People are the weakest point
- Most organisations are victims of Phishing Attacks.
- Culture of questioning. Top down
- Training on at home risks
- Training on the different types of threats

TRAINING

- Phishing Simulators can be good educators
- Individual or Classroom style sessions
- Catered to your organisation

COMMON QUESTIONS

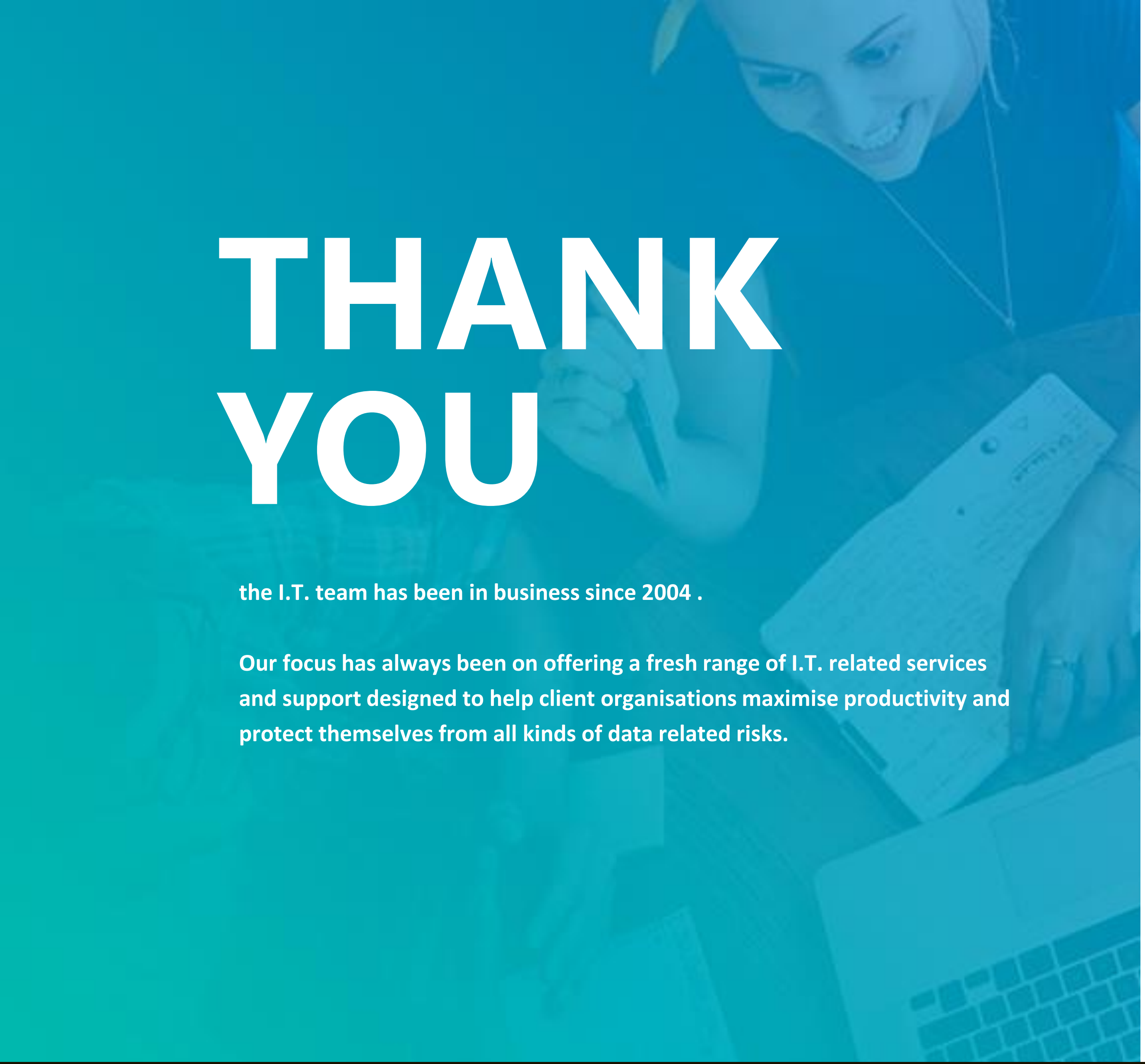
- What's single most impactful thing we could do today
- Would you recommend Teams or Zoom for remote working?
- How important is antivirus?
- How important is DNS Filtering (Cisco Umbrella, Open DNS)
- What about Backups? (and Office 365 Backups)

the I.T. team™

Maintaining the health of your I.T. system

QUESTION TIME

webinar@theitteam.co.nz



THANK YOU

the I.T. team has been in business since 2004 .

Our focus has always been on offering a fresh range of I.T. related services and support designed to help client organisations maximise productivity and protect themselves from all kinds of data related risks.

the I.T. team™

Maintaining the health of your I.T. system

theitteam.co.nz

HOW TO PREVENT PHISHING ATTEMPTS

- **Check the sender's email address.** Are they who they claim to be? Check that their contact name matches the actual email address they're sending from.
- **Try not to click or tap!** If it's a link and you're on a computer, take advantage of your mouse's hover to closely inspect the domain address before clicking on them.
- **Try not to download files from unfamiliar people.** Avoid opening attachments from any external email addresses or phone numbers.
- **Get someone else's opinion.** Ask a co-worker: Were we expecting an email from this sender? Or ask a friend: Does this email look strange to you? A good practice is to use a *different medium* to verify (for example, if you receive a strange email claiming to be your friend, try calling your friend over the phone to double-check that it's from them).

HOW TO PREVENT PHISHING ATTEMPTS

- Protect your passwords and login credentials, don’t enter these into any websites relating to the COVID-19 virus
- Keep your devices up-to-date
- Keep your anti-virus up to date and run regular checks