



Avon & Somerset Police Cyber Protect

Kristian Evans – COVID19 Presentation

24 March, 2020

Sources



National Cyber
Security Centre
a part of GCHQ



SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit



TO STOP FRAUD™

Action Fraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

CYBER AWARE 

Useful (only slightly technical) Links



www.lifewire.com

www.howtogeek.com

www.ncsc.gov.uk



Background – COVID-19



SCAM WARNING

Coronavirus-related frauds increase by 400% in March

Between 1st February 2020 and 18th March 2020, Action Fraud has received **105 reports** from victims of coronavirus-related frauds, with losses totalling close to **£970,000**. The majority of the reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived. We have also received over **200 reports** about coronavirus-themed phishing emails attempting to trick people into opening malicious attachments or revealing sensitive personal and financial information.

Watch out for scam messages:
Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details

Shopping online: If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. Where possible, use a credit card to make the payment, as most major credit card providers insure online purchases.

Protect your devices from the latest threats:
Always install the latest software and app updates to protect your devices from the latest threats.

SCAM WARNING

Face Mask Anti-Virus

Anti Coronavirus Disease (COVID-19):
Profession Disposable Medical Mask & KN95 Face Mask is Available Now!

Subject: COVID-19 Solidarity Response Fund for WHO - DONATE NOW

We are all affected by the growing COVID-19 pandemic. It's an unprecedented health challenge and we know people and organizations every Organization is leading and coordinating the global effort, supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared, especially those with the weakest health systems. **Donations support the greatest need right now is to help ensure all countries are prepared, especially those with the weakest health systems. Donations support to develop vaccines, tests, and treatments.**

Now you can help us by donating any amount you want with the help of BITCOIN NETWORK

DONATE NOW with Bitcoin payment

World Health Organization bitcoin address (BTC Wallet) for donations is: 39w2TUFxgYKNUjpZBF54X3Dcf8RV7zoLM

Your contribution will matter!

© 2020 WHO

World Health Organization

Anti Virus Profession Medical Mask & Order Now Ship Out Within 12 Hours!

Active Since

Get It Now

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (rebate) of 128.34 GBP.

[Access your funds now](#)

The funds can be used to protect yourself against COVID-19(<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)



Ransomware Case Study



Case Study



- WannaCry

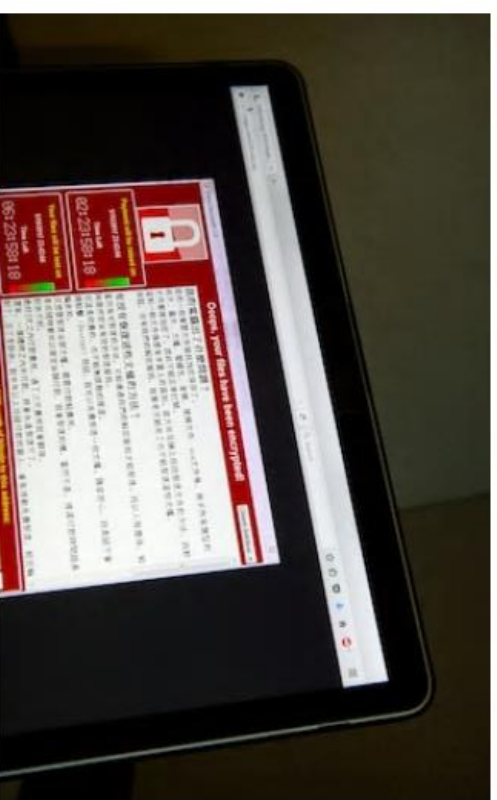
- American secret agencies being shady like in the Bourne movies
- Russian bad guys
- North Korean bad guys
- An underdog British hero good guy
-but maybe bad guy.

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled



Save 4



A computer hit by the WannaCry attack. credit: AP

Case Study

CYBER WARFARE

An NSA cyber weapon is reportedly being used against American cities by the very adversaries it was meant to target

By Jared Keller | May 25, 2019 at 02:07 PM

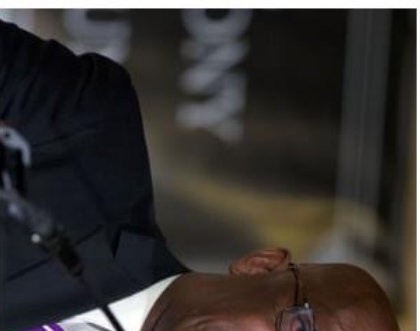
MILITARY TECH

f Share | v Share | in Share | e Share



Baltimore: government computers crippled by attack as hackers demand bitcoin

Attack on city computers prevents employees from sending email and knocked out bill pay websites, as hackers demand \$76,000



▲ Baltimore's mayor, Bernard C. 'Jack' Young, said: 'We

Meghna/AP

Hackers have seized control of gover
Baltimore, demanding ransom and li
technology for more than two weeks

Second US town pays up to ransomware hackers

2 hours ago

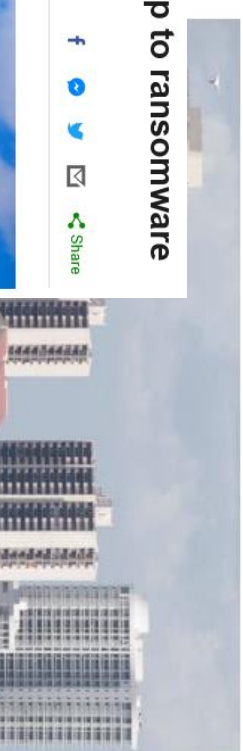


More than one town in Florida has been

A town in Florida has paid \$500,000
attack.

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000

f | v | e | Share



Coordinated Ransomware Attack Hits 23 Texas Government Agencies



Author:
Lindsey O'Donnell
August 19
2019 | 9:38 am

3 minute read

Write a comment

Share this article:

f | v | e | ...



ment after



Vulnerabilities and Protection



Protecting Your Credentials - Passwords



iloveyou 000000 123456a

qwertyuiop password1 1111111 123456789

123123 monkey password qwerty

12345678

1234567890

1234567

abc123

dragon

123321

1q2w3e4r5t

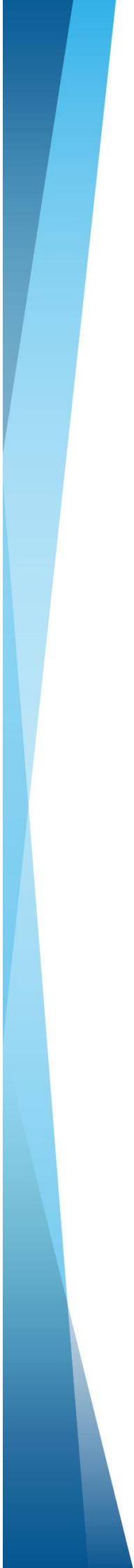
666666

654321

www.howsecureismypassword.net

Protecting Your Credentials - Passwords

- Add complexity
- MnistF.In2001bmfc
- 3 random words



Protecting Your Credentials - Has your personal information been leaked?



Largest collection ever of breached data found

Store of 770m email addresses and passwords discovered after being put on hacking site



▲ Security experts said the breach underscored the need to use password managers. Photograph: Andrew Brooks/Getty Images/Cultura RF

Alex Hern

✉ @alexhern

Thu 17 Jan 2019 17:31 GMT

A screenshot of the 'have i been pwned' website. The interface is dark blue with white text. At the top, it says "';--have i been pwned?" in a large, rounded box. Below this, it says "Check if you have an account that has been compromised in a data breach". There is a white input field labeled "email address" and a button labeled "pwned?". At the bottom, it says "Generate secure, unique passwords for every account" with a link "learn more at: 1Password.com". There is also a small icon of a person in a circle and the text "Why 1Password?".

www.haveibeenpwned.com

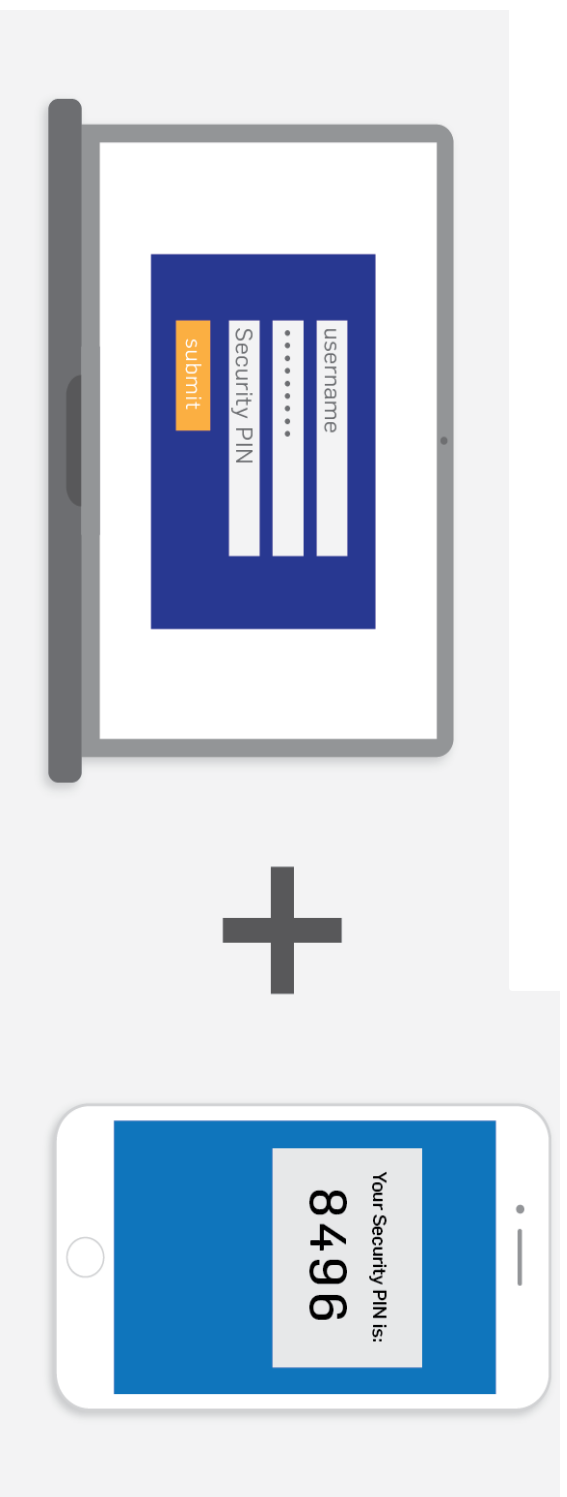
Protecting your Credentials - Password Managers



LastPass...|



Two-factor Authentication



<https://twofactorauth.org/>

2FA



LastPass...

Mobile Device



- Don't lose
- Lock-screen
- Find my phone
 - Google.com/android/find
 - Icloud.com/find
- Remote Wipe
- Back-Up
- Encryption
- Back-up
- 2FA & password managing
- Only use the proper app stores





Firewalls Software-Updates Anti-Virus



Firewalls



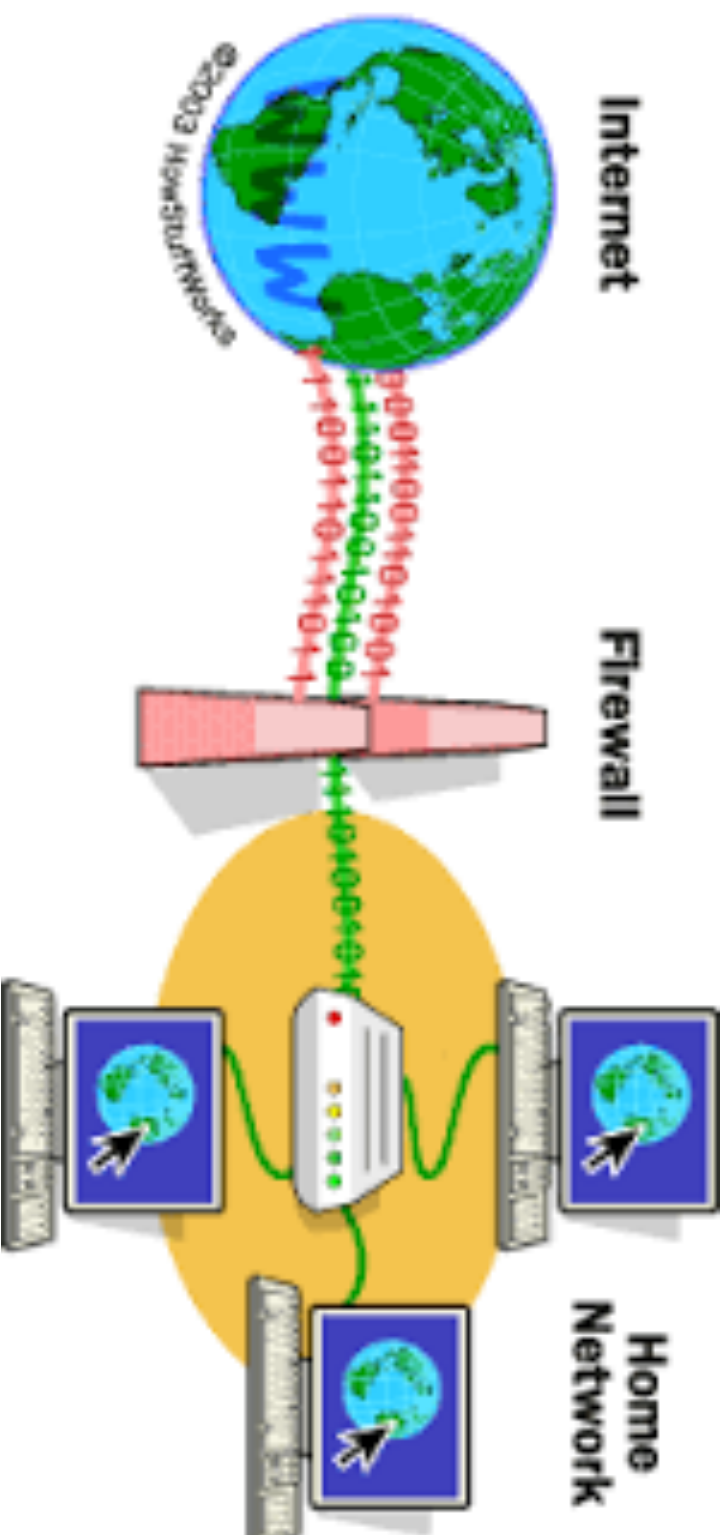
- Turn them on!



Firewalls



- Protect Your environment!

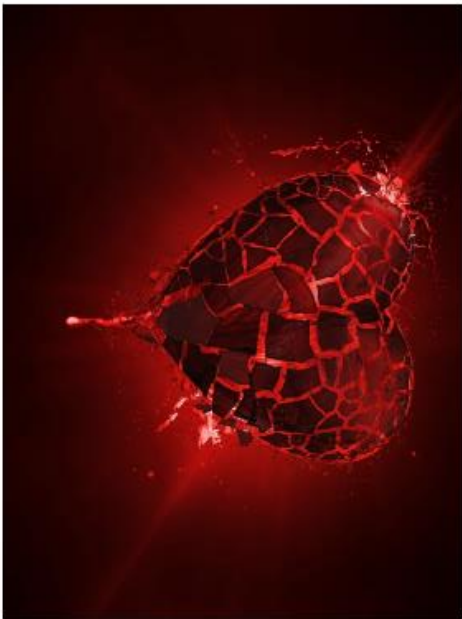


Anti-Virus/Anti-Malware

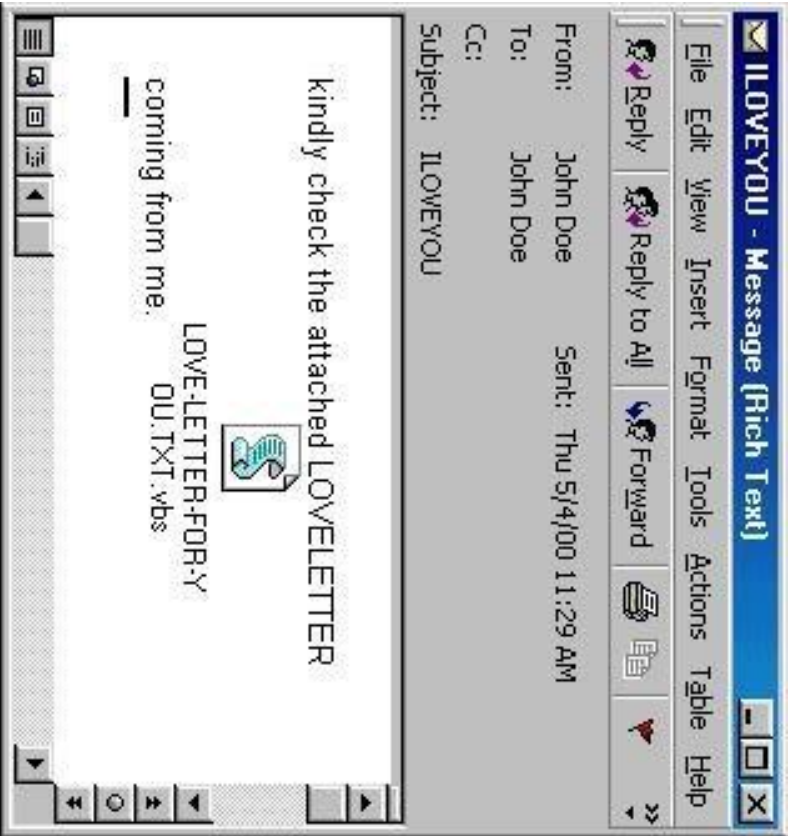
Tales In Tech History: 'I Love You' Virus

Tom Jowitt, June 2, 2017, 8:42 am

CYBERCRIME SECURITY



The 'I love you' worm had a devastating impact on computer networks worldwide seventeen years ago



Anti-Virus/Anti-Malware



Software Updates



[HOME](#)
[NEWS](#)
[S](#)

Technology Intelligence

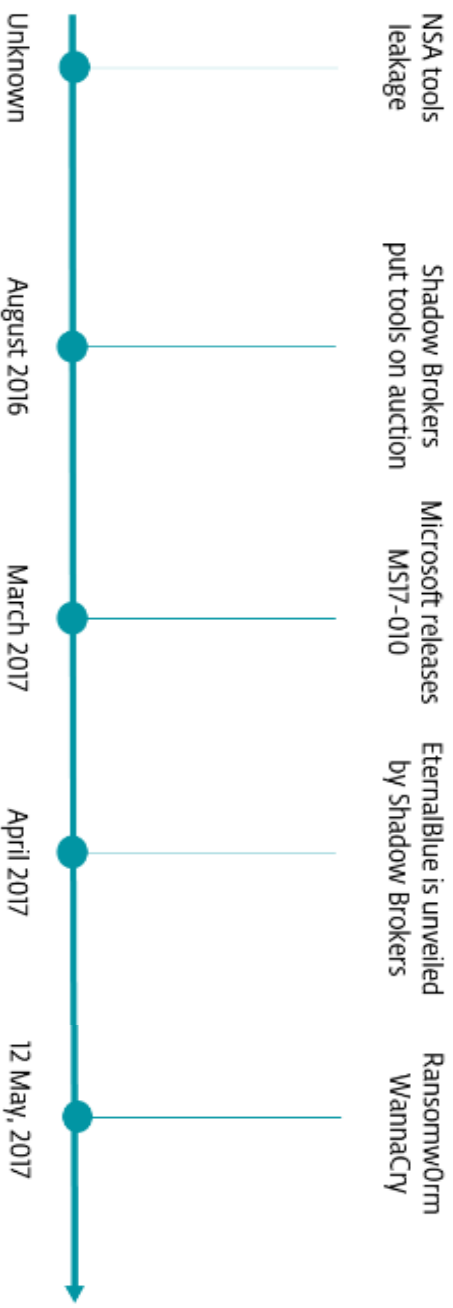
[Gadgets](#)
[Innovation](#)
[Big Tech](#)
[Start-ups](#)
[Politics of Tech](#)
[Gaming](#)
[Podcast](#)
[T](#)

Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled

[f share](#)
[t](#)
[e](#)
[4](#)

A computer hit by the WannaCry attack - credit: AP



Backing Up



- File Back-Up
 - Cloud Options
 - Windows File History
- System Imaging



Reporting



Action Fraud
customer channels



Social Media

Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.



0300 123 2040

Report fraud and cyber crime.
Help, support and advice.

Report 24/7 & Web Chat

www.actionfraud.police.uk

Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

24/7 live cyber

Specialist line for business, charities or organisations
suffering live cyber attacks

National Fraud and Cyber Crime
Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance



Phishing During the Outbreak



Phishing



- The No.1 method of creating a victim.
- After the initial 'Phish' there are a wide range of options open to attackers.
- Think – Take 5



Phishing



- Techniques used to phish you in
 - Urgency
 - Authority
 - Entitlement
 - Bullying
 - Charisma
 - Trust
 - Reward
 - Curiosity





Mon 4/29/2019 10:57 AM

officialfbi@usa.com

Attention: Beneficiary

To:

We removed extra line breaks from this message.

OFFICIAL LETTER FROM FEDERAL BUREAU OF INVESTIGATION FBI

EXECUTIVE DIRECTOR FBI FEDERAL BUREAU OF INVESTIGATION

FBI, WASHINGTON DC.

FBI Director

FBI SEEKING TO WIRETAP INTERNET

Dear:Beneficiary,

We the Federal Bureau of investigation (FBI) through our intelligence-monitoring network have discovered that the transaction that the bank contacted you previously for was legal. Recently the fund has been legally approved to be paid via Bank of America. So, we the Federal Bureau of investigation (FBI) Washington Dc, in conjunction with the United Nations (UN) financial department have investigated through our monitoring network noting you that your transaction with the Bank of America is legal.


You have the legitimate right to complete your transaction to claim your fund \$10.7 (Ten million seven hundred thousand united state dollars) Because of so much scam going on internet. We the Federal Bureau of investigation decided to contact the CARGO LOGISTICS COURIER DELIVERY SERVICE, for They to give us their procedures on how to send this money to you without any further complain or delay. We just got an information from the Bank of America and they have loaded your \$10.7 (Ten million seven hundred thousand united state dollars) in CHECK and submit to the CARGO LOGISTICS COURIER DELIVERY SERVICE for immediate delivery to your doorstep. You are required to choose one option, which you will be to pay and also convenient for you,For quick delivery of your parcel containing your "CHECK" and other two original back up documents.

We request that you reconfirm your mailing address to ensure conformity with our record for immediate dispatch of your parcel to you. Only valid residential/Office address and postal address are certified OK.

Spam email



From: customerservice@secure.com
To:
Sent: 18/03/2014 08:49:51 GMT Standard Time
Subj: Important information: Your account maintenance

**NatWest**
Helpful Banking

Dear Customer,

Your internet banking access has been suspended in order to protect your account against possible misuse.

You must click the link below to reinstate your account.

<https://www.nwoblb.com/default.aspx?referident=A36989F55966CD>

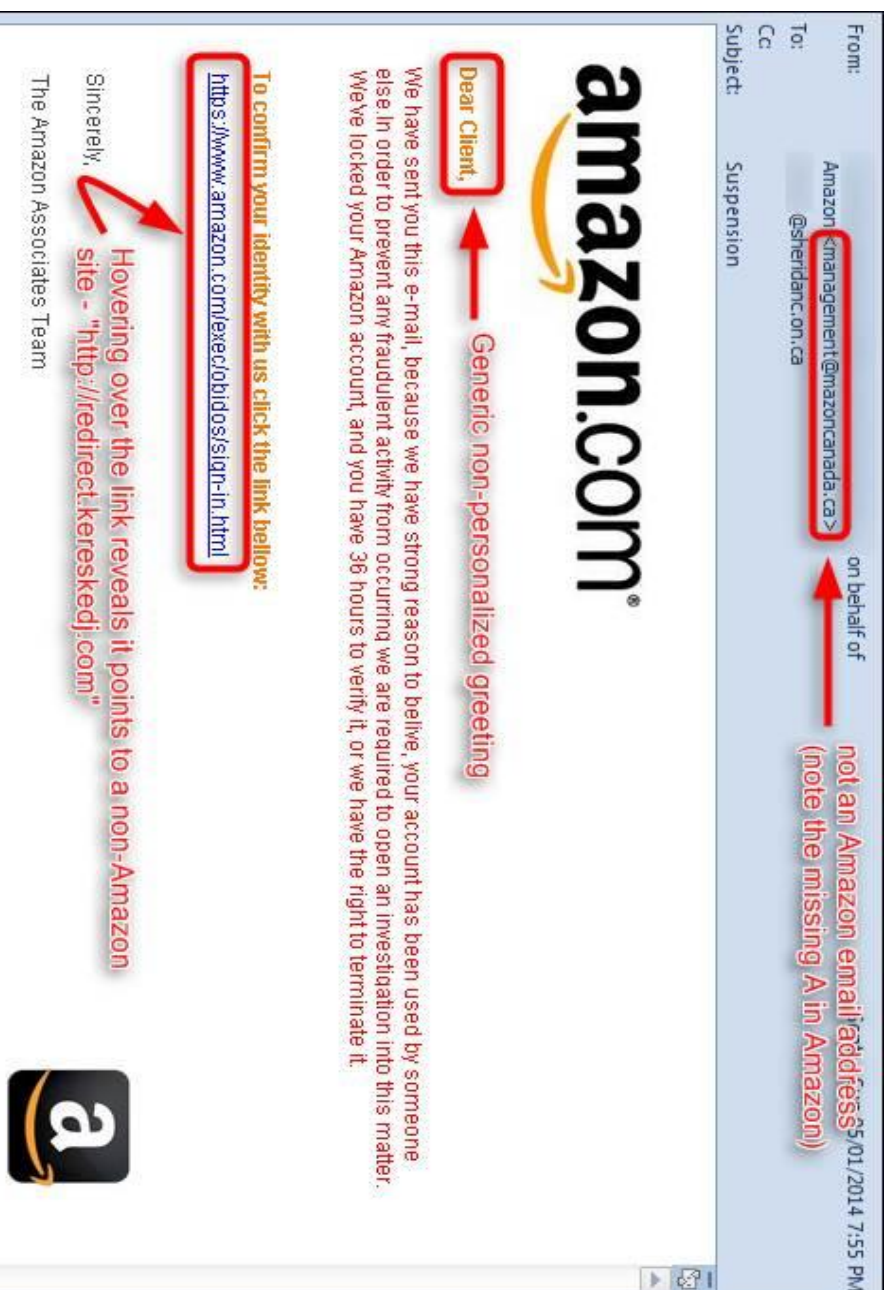
Don't hesitate to fill correctly your details, but please do respond to this email on time to avoid possible data loss.

Please accept our apologies for any inconvenience this action may have caused.

Sincerely,

Shoomon Perry
Internet support team
National Westminster Bank Plc

Spam email



Let's Go Phishing



Mac Maccallister <Vansweb@mail.com>

☐ Frazer Keith

Working Together in North Somerset

Retention Policy 1 Year Inbox (1 year)

Expires 27/06/2020

Dear Ruth,

Thank you for your work supporting communities in the North Somerset area.

As you are no doubt aware VANS are a purely voluntary organisation dedicated to bettering the lives of vulnerable people in the South West. I think there are some considerable areas of interest in which VANS and NSPF could work together to deliver better services.

We have recently received significant funding from Somerset County Council to deliver community projects in our area. We have already received a high degree of interest and in order to limit this to a manageable level only the first 50 organisations to register will be considered.

In order to be considered please register with us at the link below. We will shortly follow up with an email and the grant application forms.

<http://vans.vcbroker.org.uk/volunteer/register>

Lee Vittoff

Phishing Officer

W: vansweb.org.uk



Weston Court, Oldmixon Crescent, Weston-super-Mare. BS24 9AU

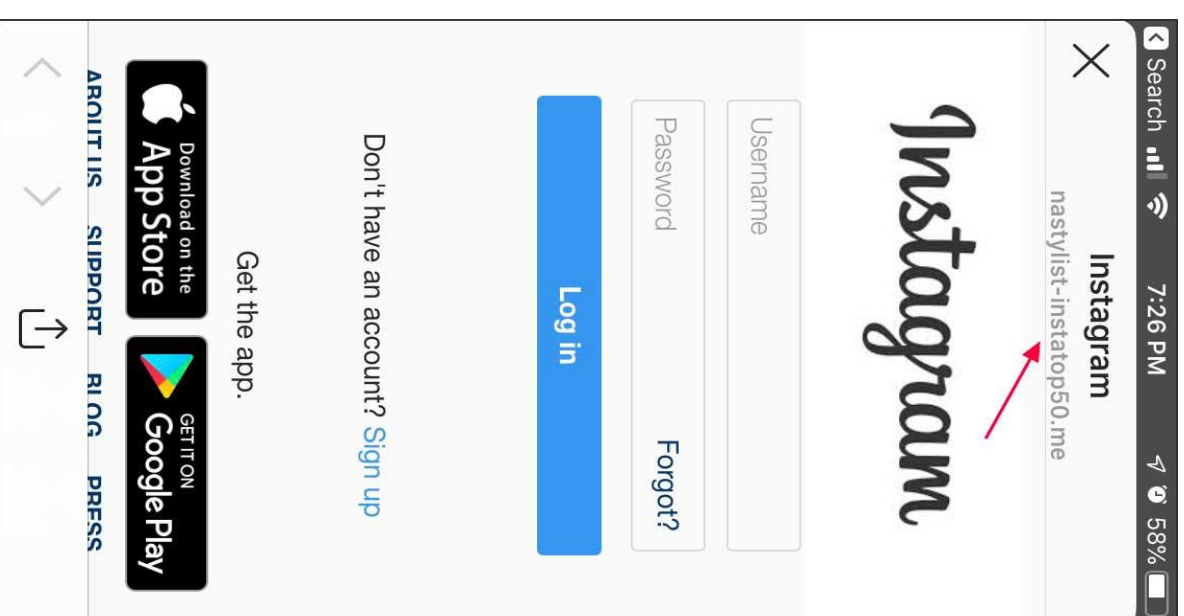
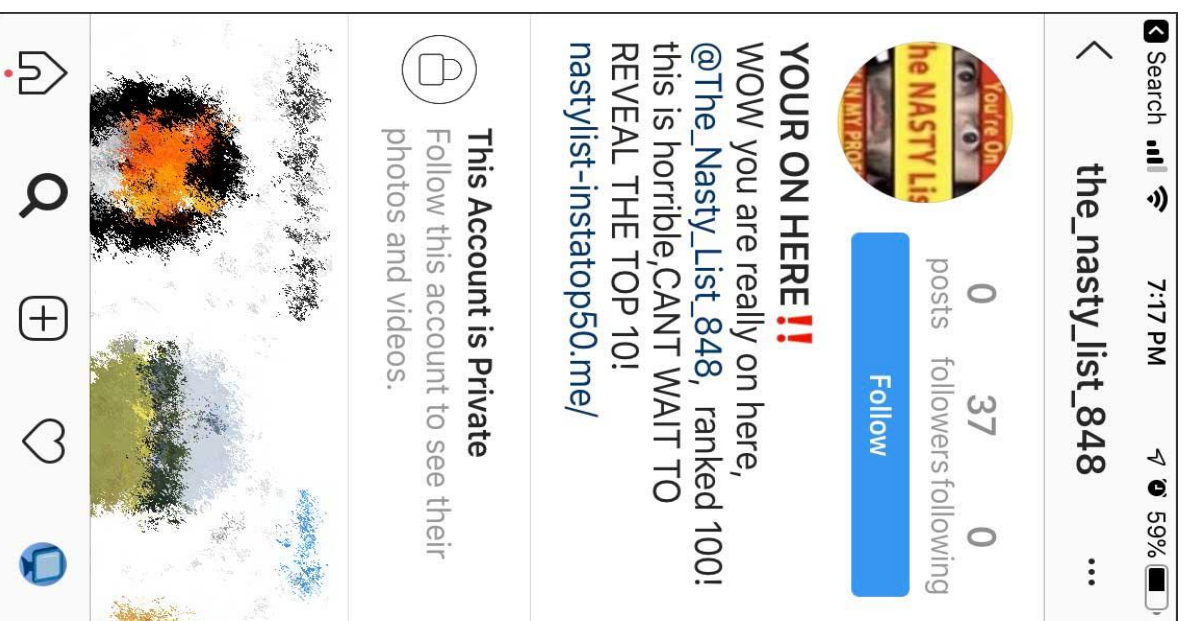
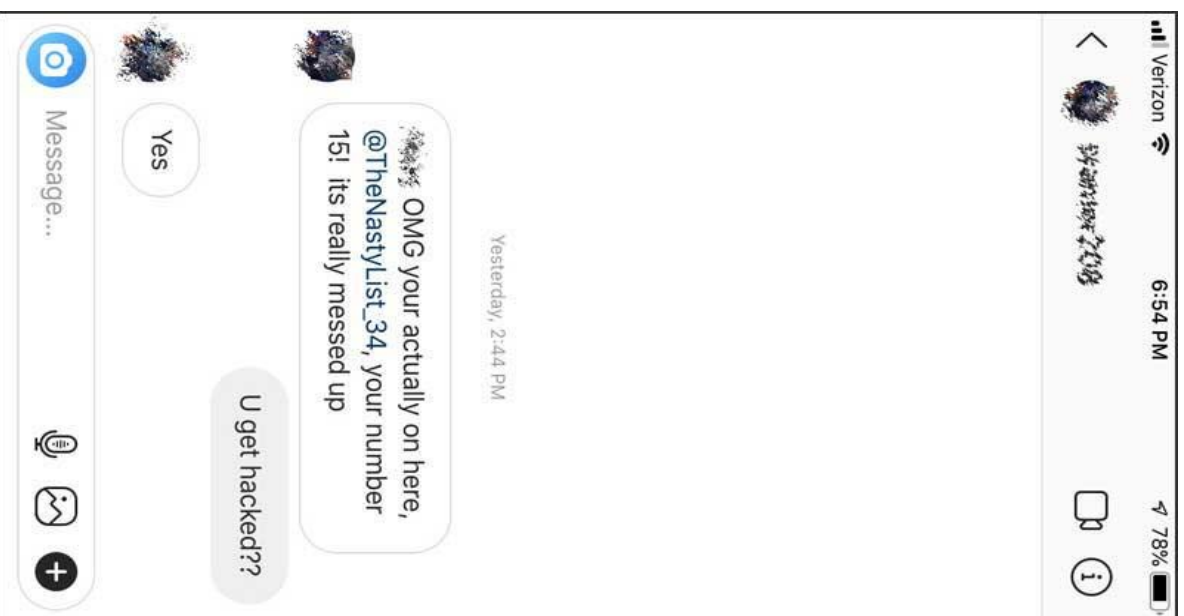
Registered Charity No: 1065916 - Company Limited by Guarantee No: 3466492

We have recently received significant funding from Somerset County Council to deliver community projects in our area. We have already received a high degree of interest and in order to limit this to a manageable level only the first 50 organisations to register will be considered.

In order to be considered please first register at <http://www.naughtydomain.com>. We will shortly follow up with an email and the grant application forms.


Click or tap to follow link.

<http://vans.vcbroker.org.uk/volunteer/register>






Mobile Phishing



**Customer**
@Customer



Follow

Hey @YourCompany why can't I login to my account? Fix it please!!



 Reply  Retweet  Favorite  More

2:51 PM - 25 Feb 19 - Embed this Tweet

**Fake Company**
@FakeCompany

Follow

@Customer Dear Customer, we are sorry that this has happened. Login to your account at www.fakecompany.com

 Reply  Retweet  Favorite  More

Phishing – Have you been caught out?



- You start getting lot of emails
- Unsolicited 'Anti-Virus' scans start cropping up
- Emails or phone calls from 'Microsoft'
- New browser toolbars
- Redirection from websites and excessive pop-ups
- Messages to friends and contacts
- Passwords not working
- New software is installed
- You're missing money
- Your computer is a brick

Take 5



- *Never disclose security details, such as your PIN or full password* – it's never right to reveal these details
- *Don't assume an email request or caller is genuine* – people aren't always who they say they are
- *Don't be rushed* – a bank or genuine organisation won't mind waiting to give you time to stop and think
- *Listen to your instincts* – if something feels wrong then it is usually right to pause and question it
- *Stay in control* – have the confidence to refuse unusual requests for information





Working From Home

Making your home cyber safe



- Change default passwords
- Install antivirus
- Review app permissions
- Use strong passwords
- Back up your data
- Review privacy settings for your social media accounts





Online fraud

Being safe online



- Follow the advice given
- Passwords
- Phishing awareness
- Create backups
- Encrypt data
- Don't click links from unknown senders
- Use password managers
- 2-Factor Authentication
- Turn on Antivirus/Firewalls
- Report all cyber crimes





Summary

Being safe online

- Ransomware
- Phishing
- Working from home (WFH)
- Wider online fraud



MAKE YOUR HOME A CYBER SAFE STRONGHOLD



Wi-Fi: always
change the default
router password



Install antivirus
software on all
devices connected
to the internet



Review your apps'
permissions and
delete those you
don't use



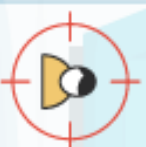
Choose strong and
different passwords
for your email and
social media
accounts



Back up your data
and run regular
software updates



Secure electronic
devices with
passwords, PIN or
biometric
information



Review the privacy
settings of your
social media
accounts



CARING



COURAGEOUS



INCLUSIVE



LEARNING

Stay alert and don't:

⊗ Reply to suspicious messages or calls



⊗ Open links and attachments in unsolicited emails and text messages



⊗ Share your bank card details or personal financial information



⊗ Share news that doesn't come from official sources

⊗ Make donations to charities without double-checking their authenticity

⊗ Buy things online that seem to be sold out everywhere else

⊗ Send money upfront to someone you don't know



CARING



COURAGEOUS



INCLUSIVE



LEARNING



Online shopping safety tips



Buy from **reliable** online vendors and check individual ratings



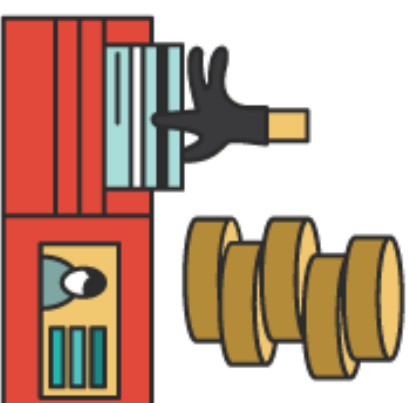
Use **credit cards** when shopping online for stronger customer protection



Think twice: if an offer sounds too good to be true, it probably is



Check your bank account often for **suspicious activity**



CARING



COURAGEOUS



INCLUSIVE



LEARNING

Cyber safety with children



Check the **security** and **privacy** settings of smart toys

Use **parental controls** to safeguard your child's online activity

Change the default factory **password** and keep software up-to-date

Talk to your child about cyber safety. **Listen** to their online experiences and **explain** to them the importance of being just as safe online as offline

REMEMBER

Follow trusted sources for up-to-date factual information. If you become a victim of cybercrime, always report it to your national police.



CARING



COURAGEOUS



INCLUSIVE



LEARNING

Websites

- <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold>
- <https://www.lifewire.com/>
- <https://www.howtogeek.com/>
- <https://takefive-stopfraud.org.uk/>
- <https://www.saferinternet.org.uk/>
- <https://www.ncsc.gov.uk/section/information-for/individuals-families>
- <https://www.actionfraud.police.uk/>



CARING



COURAGEOUS



INCLUSIVE



LEARNING