# Cyber Resilience COVID-19 Bulletin

ISSUE: 02.07.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Scottish Government
Riaghaltas na h-Alba
gov.scot

# Cyber Resilience COVID-19 Bulletin

**As a result of the significant rise in COVID-19 related scams, over the next few months the Scottish Government Cyber Resilience Unit will share important information on current cyber resilience issues. We aim to update the Bulletin on a weekly basis and ask that you consider circulating the information to your networks, adapting where you see fit. Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from trusted sources.**

**This Bulletin is also available online here. Please note the next Bulletin will be available on 16th July 2020. (There will be no Bulletin on Thursday 9th July.)**

## National Cyber Security Centre (NCSC): Remote working

The NCSC have launched a new ‘Home and Remote Working’ scenario for their Exercise In A Box tool. This is a free tool that helps organisations test and practise their response to a cyber attack. This new scenario looks at the events that take place when employees need to work remotely at short notice and helps to minimise the risks of data compromise. To use Exercise in a Box you need to register for an account. This enables the NCSC to provide you with a tailored report, helping you identify your next steps and pointing you towards the guidance which is most relevant for your organisation.

The Suspicious Email Reporting Tool allows members of the public to report suspicious emails to the NCSC.

NCSC produce weekly threat reports drawn from recent open source reporting. View this week’s report here.

## Trending Topics

### Zoom will offer end-to-end encryption for all users

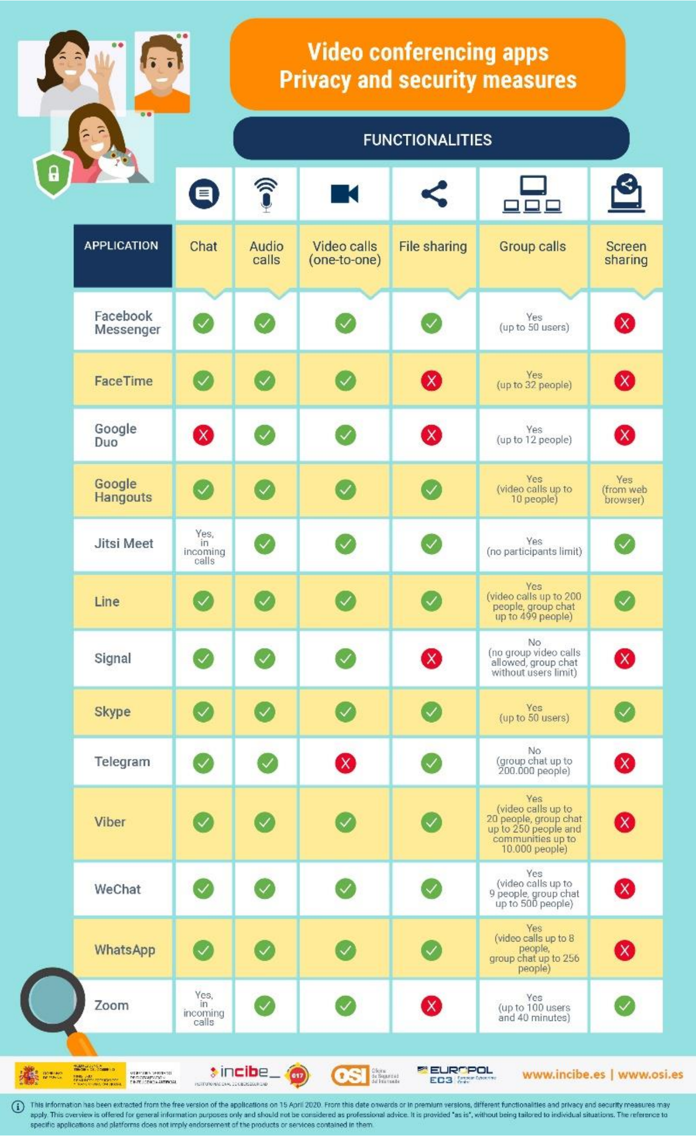
Zoom has announced that it will make end-to-end encryption (E2EE) available to all users. The news came as rights groups, tech firms and internet users petitioned the firm to reverse its policy on E2EE. Free/basic users seeking access to E2EE will participate in a one-time process that will prompt them for additional pieces of information, for example by verifying a phone number by text message. An early “beta” version is planned for July.

### Zoom credentials found online

The National Law Review has reported that it has discovered that over 500,000 Zoom accounts were sold on the dark web in April. Cyble, a cybersecurity firm, were able to purchase approximately 530,000 Zoom credentials, including each user’s email address, password, meeting ID, and meeting URL. Some of the accounts were confirmed to belong to various universities and banks around the world. These accounts are not believed to have been breached from Zoom itself, but rather discovered as the owners of the accounts have reused the same password for a different service that was compromised. This demonstrates how important for us all to use different passwords for different accounts, as reusing passwords can result in a higher risk of an account compromise.

## Europol infographic download available here

This infographic provides information about the functionality, and privacy and security settings of a number of communication platforms.



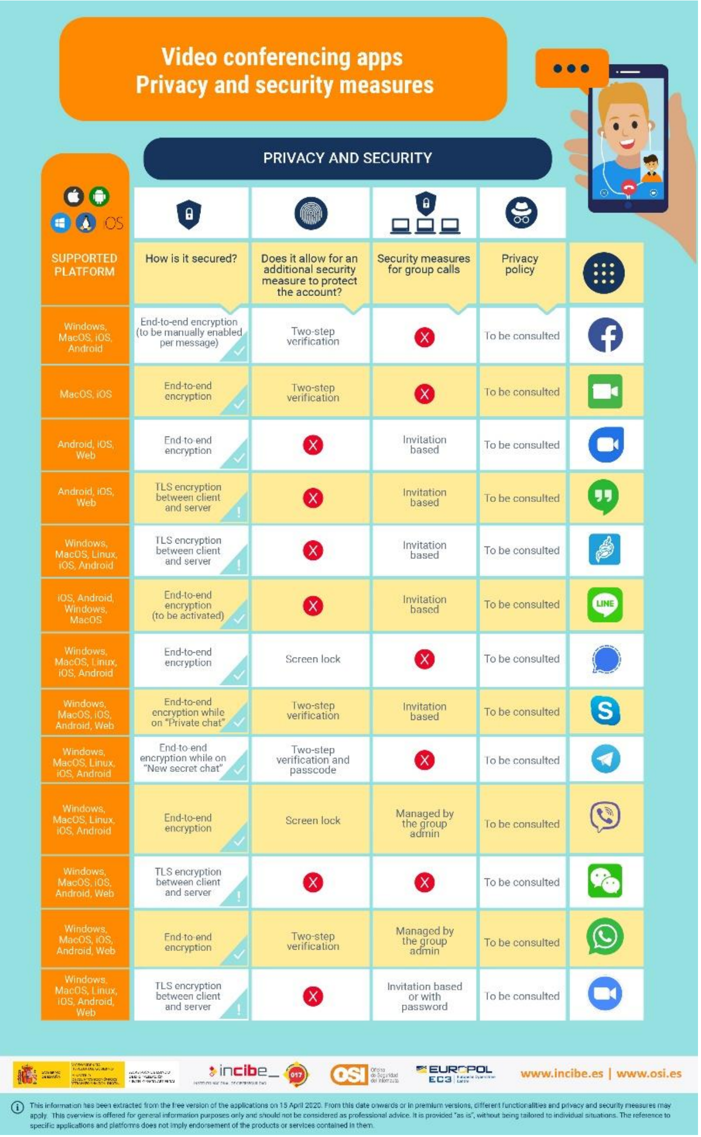
Video conferencing apps
Privacy and security measures

FUNCTIONALITIES

| APPLICATION | Chat | Audio calls | Video calls (one-to-one) | File sharing | Group calls | Screen sharing |
|---|---|---|---|---|---|---|
| Facebook Messenger | ✓ | ✓ | ✓ | ✓ | Yes (up to 50 users) | ✗ |
| FaceTime | ✓ | ✓ | ✓ | ✗ | Yes (up to 32 people) | ✗ |
| Google Duo | ✗ | ✓ | ✓ | ✗ | Yes (up to 12 people) | ✗ |
| Google Hangouts | ✓ | ✓ | ✓ | ✓ | Yes (video calls up to 10 people) | Yes (from web browser) |
| Jitsi Meet | Yes, in incoming calls | ✓ | ✓ | ✓ | Yes (no participants limit) | ✓ |
| Line | ✓ | ✓ | ✓ | ✓ | Yes (video calls up to 200 people, group chat up to 499 people) | ✓ |
| Signal | ✓ | ✓ | ✓ | ✗ | No (no group video calls allowed, group chat without users limit) | ✗ |
| Skype | ✓ | ✓ | ✓ | ✓ | Yes (up to 50 users) | ✓ |
| Telegram | ✓ | ✓ | ✗ | ✓ | No (group chat up to 200.000 people) | ✗ |
| Viber | ✓ | ✓ | ✓ | ✓ | Yes (video calls up to 20 people, group chat up to 250 people and communities up to 10.000 people) | ✗ |
| WeChat | ✓ | ✓ | ✓ | ✓ | Yes (video calls up to 9 people, group chat up to 500 people) | ✗ |
| WhatsApp | ✓ | ✓ | ✓ | ✓ | Yes (video calls up to 8 people, group chat up to 256 people) | ✗ |
| Zoom | Yes, in incoming calls | ✓ | ✓ | ✗ | Yes (up to 100 users and 40 minutes) | ✓ |

incibe_ 017 OSI Oficina de Seguridad del Internauta EUROPOL EC3 European Cybercrime Centre www.incibe.es | www.osi.es

ⓘ This information has been extracted from the free version of the applications on 15 April 2020. From this date onwards or in premium versions, different functionalities and privacy and security measures may apply. This overview is offered for general information purposes only and should not be considered as professional advice. It is provided "as is", without being tailored to individual situations. The reference to specific applications and platforms does not imply endorsement of the products or services contained in them.



Video conferencing apps
Privacy and security measures

PRIVACY AND SECURITY

| SUPPORTED PLATFORM | How is it secured? | Does it allow for an additional security measure to protect the account? | Security measures for group calls | Privacy policy | |
|---|---|---|---|---|---|
| Windows, MacOS, iOS, Android | End-to-end encryption (to be manually enabled per message) ✓ | Two-step verification | ✗ | To be consulted | f |
| MacOS, iOS | End-to-end encryption ✓ | Two-step verification | ✗ | To be consulted | |
| Android, iOS, Web | End-to-end encryption ✓ | ✗ | Invitation based | To be consulted | |
| Android, iOS, Web | TLS encryption between client and server ! | ✗ | Invitation based | To be consulted | |
| Windows, MacOS, Linux, iOS, Android | TLS encryption between client and server ! | ✗ | Invitation based | To be consulted | |
| iOS, Android, Windows, MacOS | End-to-end encryption (to be activated) ✓ | ✗ | Invitation based | To be consulted | LINE |
| Windows, MacOS, Linux, iOS, Android | End-to-end encryption ✓ | Screen lock | ✗ | To be consulted | |
| Windows, MacOS, iOS, Android, Web | End-to-end encryption while on "Private chat" ✓ | Two-step verification | Invitation based | To be consulted | S |
| Windows, MacOS, Linux, iOS, Android | End-to-end encryption while on "New secret chat" ✓ | Two-step verification and passcode | ✗ | To be consulted | |
| Windows, MacOS, Linux, iOS, Android | End-to-end encryption ✓ | Screen lock | Managed by the group admin | To be consulted | |
| Windows, MacOS, iOS, Android, Web | TLS encryption between client and server ! | ✗ | ✗ | To be consulted | |
| Windows, MacOS, iOS, Android, Web | End-to-end encryption ✓ | Two-step verification | Managed by the group admin | To be consulted | |
| Windows, MacOS, Linux, iOS, Android, Web | TLS encryption between client and server ! | ✗ | Invitation based or with password | To be consulted | |

incibe_ 017 OSI Oficina de Seguridad del Internauta EUROPOL EC3 European Cybercrime Centre www.incibe.es | www.osi.es

ⓘ This information has been extracted from the free version of the applications on 15 April 2020. From this date onwards or in premium versions, different functionalities and privacy and security measures may apply. This overview is offered for general information purposes only and should not be considered as professional advice. It is provided "as is", without being tailored to individual situations. The reference to specific applications and platforms does not imply endorsement of the products or services contained in them.

**NCSC Guidance on video conferencing**

- **Video Conferencing services: using them securely – guidance for individuals and families about the use of video conferencing software**
- **Video conferencing services: guidance for organisations – advice about how businesses can use video conferencing safely and securely**

## WhatsApp

An alert has been issued about a 'sophisticated' WhatsApp scam. Hackers have targeted thousands of profiles, telling users that their accounts need to be verified. The new version of the scam comes from a user named the "WhatsApp Technical Team". The profile picture feature the WhatsApp logo - and the account asks users to verify their identity by sending over their six-digit log-in code. In another example, the criminals will pose as a friend, saying they have accidentally sent their authorisation code over to you. This is a trick to get your own login code, which in turn will give hackers access to your account, so they can send a text to your contacts and read all of your messages.

WhatsApp never asks for your data or verification codes. To stay safe, set up two-factor authentication on your accounts, with controls usually found within your account settings. That means that even if someone gets access to your six-digit number they will still need an extra password, which adds an extra layer of security for your private details.

## Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk

Retail and non-essential shops are starting to reopen across the country, however many of us continue to shop online. Since shops were forced to close due to the COVID-19 outbreak on 23rd March, Action Fraud has received reports of online shopping fraud totalling £16.6 million in losses. This report details how members of the public purchased mobile phones, vehicles, and electronics from scam websites only for these items never to arrive. It also reveals that nearly a quarter of online fraud victims during lockdown are aged between 18 to 26. You should stay vigilant and take extra care online. The NCSC have guidance to help ensure you have a secure online shopping experience.

## Staycation – Holiday scams

Consumers are being warned about a sharp rise in COVID-19-related holidays scams, including fake caravan and motorhome listings targeting those planning a summer staycation.

Additionally, travellers whose plans have been disrupted by the COVID-19 pandemic are being targeted by scammers pretending to issue refunds for cancelled holidays. Fraudsters are impersonating airlines, travel companies and banks in order to steal personal information and money. https://www.which.co.uk/news/2020/06/travellers-warned-of-cancelled-holiday-refund-scams-this-summer/

## Newsletters

### Trading Standards scam share

Other scams to be aware of are identified in this week's Trading Standards Scotland Scam Share newsletter. You can sign up for their newsletter here.

### Neighbourhood Watch Scotland

Sign up to the Neighbourhood Watch Alert system to receive timely alerts about local crime prevention and safety issues from partners such as Police Scotland.

## Training of the week

### SBRC – How to reduce the cyber risk for Scotland's mid-market businesses

Mid-market firms are highly diverse: vulnerabilities and assets requiring protection vary. While the mid-market is a dynamic, high growth part of the economy, organisations rarely have the scale and financial resource to employ full-time cyber security teams. Directors are faced with complex investment decisions surrounding security versus growth-driving initiatives. Hear from a range of speakers on how organisations can be more effective in this area, and if incidents do arise, how to respond.

Sign up for this webinar below:

8th July 12pm

15th July 12pm

## Authoritative Sources:

- National Cyber Security Centre **(NCSC)**
- Police Scotland
- Trading Standards Scotland
- Europol
- Coronavirus in Scotland
- Health advice NHS Inform

To **report a crime** call Police Scotland on **101** or in an emergency **999.**
We are constantly seeking to improve. Please send any feedback to CyberFeedback@gov.scot

### Case Studies

We aim to bring you real-life examples of scams, phishing emails and redacted case studies. If you have had an issue and would like to share your experience and learning with others, please contact us to discuss: CyberFeedback@gov.scot. We are happy to anonymise the case study

## Case Study – Banking Push Payment Fraud

'Saffia' received a call from what she assumed to be her bank's fraud prevention unit. A very friendly-sounding man called 'Mike' told Saffia that her account was being frequently used in a city hundreds of miles away from where she stayed; but before proceeding with the call, Mike asked her to confirm the last 4 digits of her account number. At this point, Mike repeated that he didn't need Saffia's full account number or PIN as he was going to cancel her card for her own safety, and that she would get a new card in 3 days' time. To allow the card to be cancelled and a new one to be issued, Mike sent Saffia a text, which came through directly from her bank - Mike said this was so that Saffia would know that he was genuine and the call legitimate. Mike then asked Saffia to read the code from the text she'd been sent.

At that point Saffia had a feeling something wasn't right, so told Mike that she would call the bank back. At this point Mike became much more insistent, stating that he hadn't asked Saffia for her full account number or PIN and was in fact there to help her. When Saffia was clear that she was going to call the bank, Mike hung up!

Saffia then called her bank who advised her that she'd had a lucky escape and that it was indeed a scam. In fact if Saffia had read out the code to Mike which her actual bank had sent her as a warning that someone was trying to authorise a large purchase through my account - that code would have allowed Mike to proceed with the transaction and Saffia could have lost a lot of money.

**Things to remember:**

**Authorised push payment fraud** is where someone tricks you into sending them money from your account. They often do this by contacting you via phone, email or social media and pretending to be someone else – such as your bank, a contractor, an estate agent or the police.

**Take Five To Stop Fraud has advice on banking fraud on their website as well as general COVID-19 advice. Citizens Advice also has advice on banking security and fraud.**