Be Aware of Fake Zoom Video Conferencing Invitations

During the COVID-19 pandemic, the use of video conferencing technologies such as Zoom for Healthcare is increasing and cybercriminals are using this rise to their advantage.

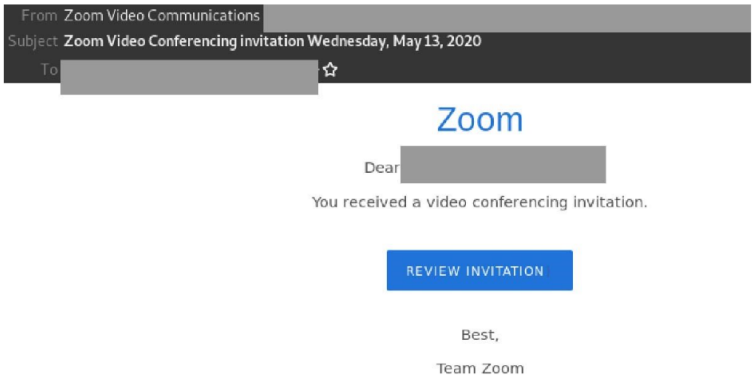
Launching cyberattacks that are centered on ongoing trends isn't new. Cybercriminals have long employed tactics to take advantage of disruptions, vulnerabilities or uncertainties to get the better of people who might not pause to check for the legitimacy of these emails. Cybercriminals also ramp up attacks during events such as holidays when people are distracted.

The following email spoofing Zoom aims to trick users into handing over their confidential details. **Zoom will never request any personal information.** It is recommended that users access this technology via the Zoom client/app rather than a web browser to connect to calls.

Using a display name of "Zoom Video Communications", the email is titled "Zoom Video Conferencing invitation Wednesday, May 13, 2020". The body of the message is addressed to the email address displayed in the "to: field", and informs recipients that they have received a video conferencing invitation. A button is provided to "review invitation".

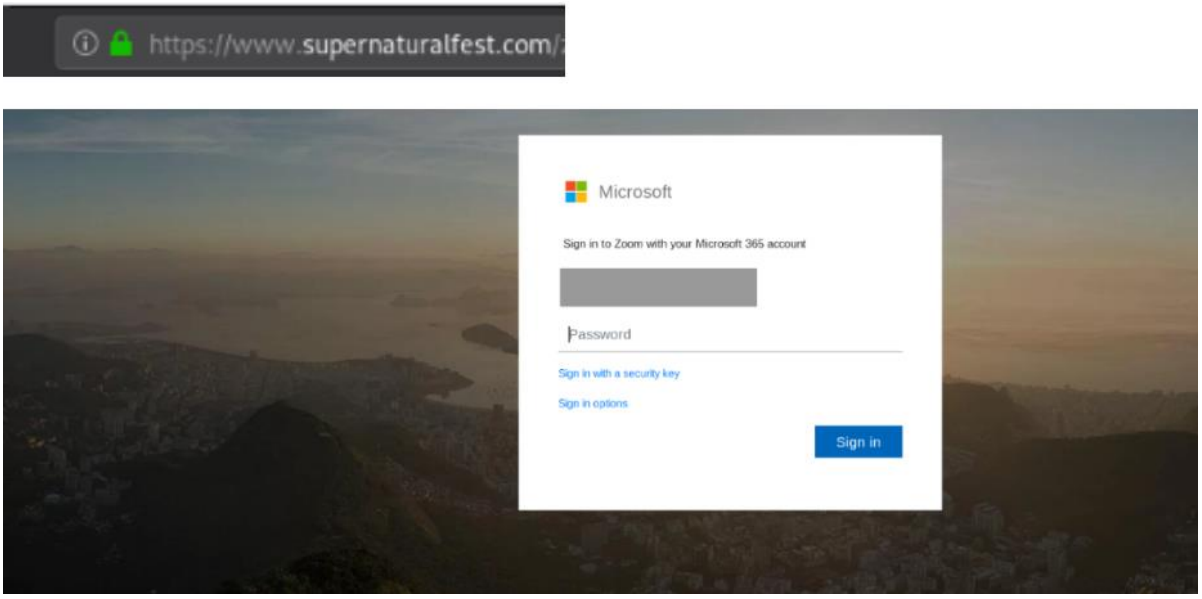
"Zoom Video Conferencing invitation Wednesday, May 13, 2020". The email actually originates from multiple randomly generated email addresses hosted on amazonses.com. The body of the message is addressed to the email address displayed in the "to: field", and informs recipients that they have received a video conferencing invitation. A button is provided to "review invitation".

Here is what the email looks like:

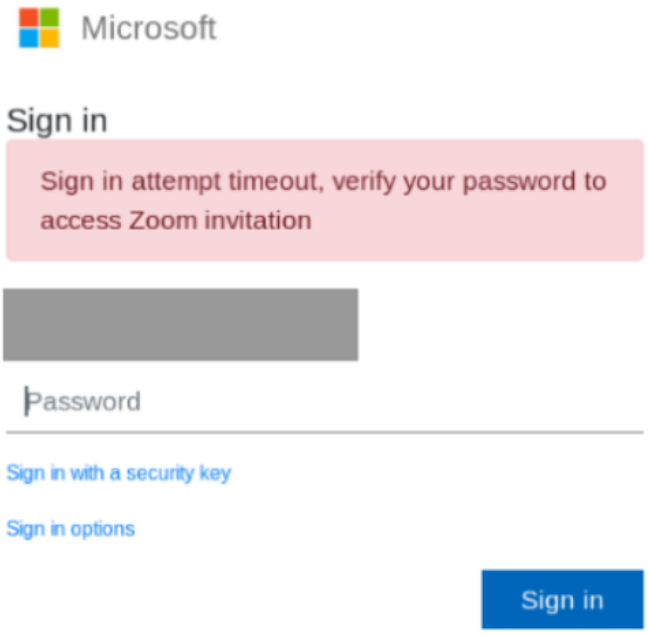


- Phishing email spoofing DHL asks users to confirm tracking number via a malicious link
- Fraudulent email uses Microsoft Excel attachment to download malicious code
- Email titled "Refund Notice" uses malicious password-protected attachment to infect systems
- Cyber-attacks on Toll Group, BlueScope, Service NSW are "just the tip of the iceberg": Alastair MacGibbon
- Phishing email titled "Final Alert" threatens to suspend user's "email service"

Unsuspecting recipients who click on the email are led to a fake Microsoft-branded login page, and asked to “sign in to Zoom with your Microsoft 365 account”. Interestingly, this page is not hosted either on a Zoom or a Microsoft domain, as per the below:



Upon “logging in”, another message appears, telling users to verify their password due to a “sign in attempt timeout”:



After inserting their password a second time, users are led to another page informing them that "this video conferencing has been cancelled". After a few seconds, they are redirected to the legitimate Zoom homepage.

This video conferencing has been cancelled

You will be redirected to zoom.
What's this?

This is a good example of how cybercriminals are leveraging the uncertainty posed by COVID-19 and its implications on the way we communicate and work. **If you receive one of these emails, or similar, please delete it immediately without clicking on any links.**

Here are a few ways cybercriminals have attempted to make this email look legitimate:

- Use of a display name like "Zoom Video Communications" suggests the email is sent from an official source.
- The inclusion of the date and day in the email's subject also places it in real-time and boosts its credibility.
- Incorporating elements (like the Zoom header) in the email that are similar to Zoom's branding and logo.
- The inclusion of the Microsoft logo and its branding elements in the phishing pages further aims to convince users into thinking the email is authentic.

Despite these techniques, some recipients of this email can spot several **red flags**, including:

- The fact that phishing pages aren't hosted on a Microsoft or Zoom domain
- The email address used in the "from" field doesn't use a familiar domain.

We strongly advise being extra vigilant when you receive emails such as these and lookout for any signs that might be suspicious. As a precaution, **do not to click links in emails** that:

- Are not addressed to you by name.
- Appear to be legitimate but use poor English or omit personal details that a legitimate sender would include.
- Are from businesses or people that you were not expecting to hear from.
- Take you to a landing page or website that is not the legitimate URL (web address) of the company the email is claiming to be sent from.

Cybercriminals know people can be tricked; that's why they send out millions of scam messages and put so much effort into making them look convincing. If scammers can trick one person into clicking on a malicious link they can gain access to our data.

We aren't perfect and can make mistakes; however, we all need to be on guard against these cyberattacks so we can protect the health information of our patients and clients as well as our clinical information systems that we rely on to deliver timely, high quality care.