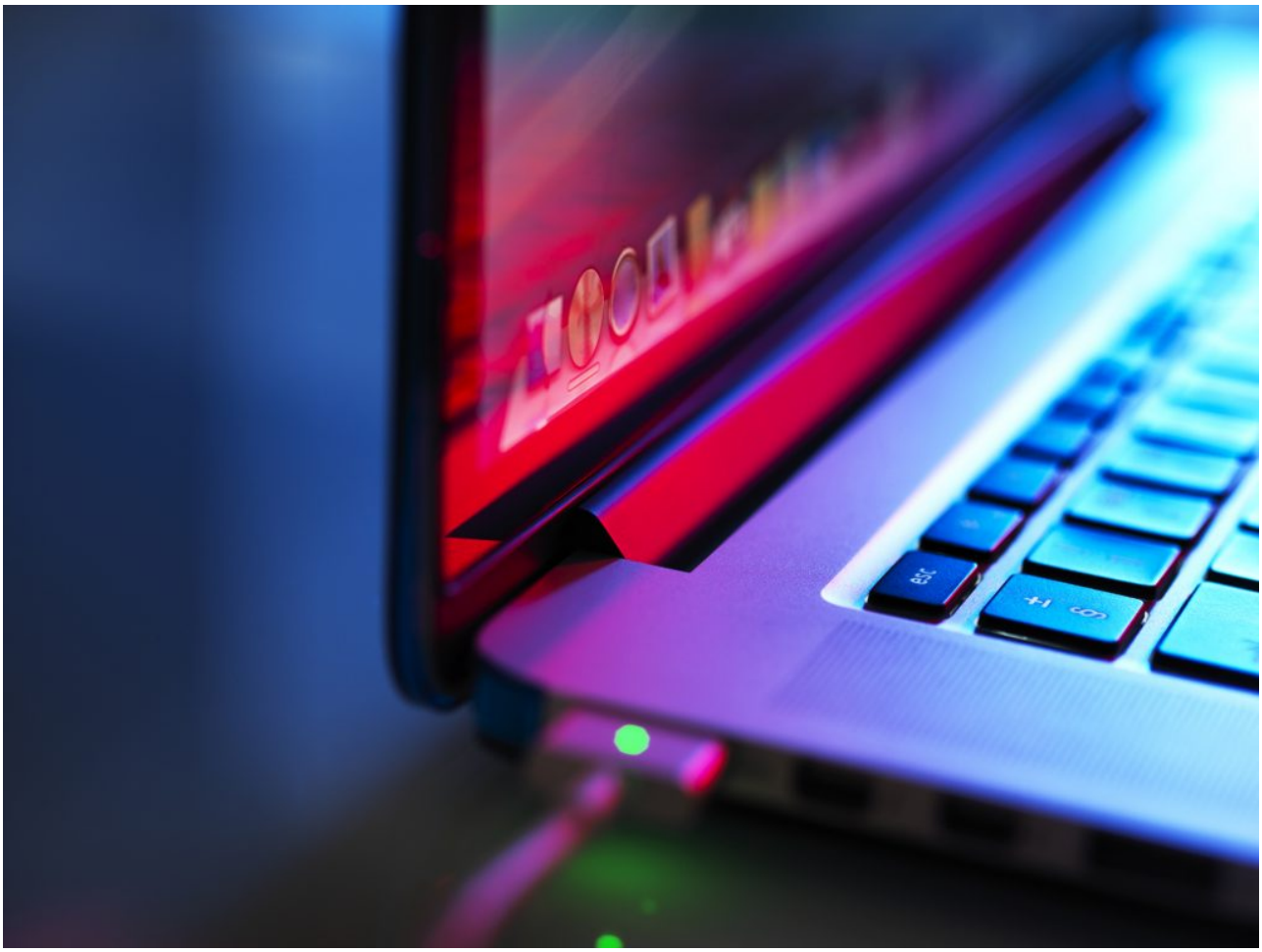
What's next

Life at Nuance

Hey Mom, I Just Called to Say ILOVEYOU

Here at Nuance, the Global Security team's mission is to ensure employees and customers are safe and secure. From the ILOVEYOU phishing attack 20 years ago, to those that continue today, we work hard to keep cybercriminals away from our networks and the sensitive information contained within. One way we do this effectively is to protect and empower our human operating system – the thousands of employees who work at Nuance – with a combination of security awareness and education content, phishing simulations and training, and an easy way to report suspicious emails to our Security Operations Center.

Leslie Nielsen
Posted February 14, 2020



In early May 2000, I was presenting my company's products at a smart card conference in Miami Beach. The gentleman in the booth next to me was in the middle of a demonstration of his company's email security product.

Live on the big screen, in front of attendees, his computer was hit by the "ILOVEYOU" virus – which today we call malware (short for "malicious software"). After watching his machine flip out, I knew there was a single defense to make it stop – we unplugged his modem.

The irony that this happened during his presentation about securing emails was not lost on anyone present.

The Power of ILOVEYOU

Back then, ILOVEYOU was one of the first and most successful phishing attacks of its kind. Also known as "Love Letter" or "Love Bug", the malware presented itself within an email with the subject line "ILOVEYOU". The email contained an attached file called "LOVE-LETTER-FOR-YOU.txt.vbs".

Victims of this phishing attack made the common mistake of not taking note of the unfamiliar

file extension at the end. When people clicked on the attachment, the malware launched itself, caused harm by overwriting files, and pulled every email address from the infected computer's Windows address book. It then morphed back to its original email format, with the attachment, and sent itself to everyone in that address book.

It was very efficient and traveled fast. Just like successful phishing campaigns we see today.

How We Secure the Human Operating System

At Nuance, we take security very seriously. My team's mission is to ensure the safety and security of Nuance and our customers.

One of the unique aspects to manage is our human operating system (human OS) – the thousands of people who work here. You can't patch the human OS or take it offline, but you can put protective measures to help prevent innocent mistakes. Here are my top three:

First, if it's on my network, it stays on my network

In our personal lives, we move and store files and data to the cloud. At Nuance, the only cloud available is the one that we can confidently secure and manage, often with key partners like Microsoft and its Azure platform.

To this end, we block employee access to suspicious websites, as well as those where information can be shared our stored (e.g. Dropbox and Google Drive). Our email security tool keeps several million unwanted emails at bay while monitoring for emails that might get sent to personal accounts.

Second, if you want to access my systems, you better be legit

All Nuance we use two-factor authentication technology to secure access to our systems, network, and data centers. This simple technology requires something you know, and something you have. In this case, what you know is your password, and what you have is a software app that generates a unique 6-digit passcode every 60 seconds.

Third, we empower good decisions with security education and awareness

We use lots of security content and technology to reach every employee, make them aware, and educate them. Our Outlook email ribbons will display a one-click button for employees to send suspicious-looking emails to our Security Operations Center for analysis. And we launch carefully crafted phishing simulations to test our employees' knowledge and provide immediate training and resources for those who did not pass the test.

Ultimately, I know I am a successful security practitioner when I can help my own mom stay in touch – by understanding the right way, and the safest way, to use her mobile phone and email.

Mom, I wish you a happy Valentine's Day. ILOVEYOU.

Tags: phishing, privacy

About Leslie Nielsen

Leslie Nielsen, Chief Information Security Officer (CISO) at Nuance, is on a mission to keep employees and customers safe and secure. With more than two decades of cybersecurity experience, Leslie has served on many Fortune 500 steering committees, is a member of the Google CISO Advisory Board, and an invited speaker at security industry events. Prior to Nuance, Leslie held multiple executive-level positions including CISO at SAP SuccessFactors, SAP Concur, and the SAP Cloud Business Group. Leslie was a Practice Manager for IBM Security Intelligence & Operations, CTO at SOS Security, a Forsythe Company, and CISO at Premier Farnell.

View all posts by Leslie Nielsen