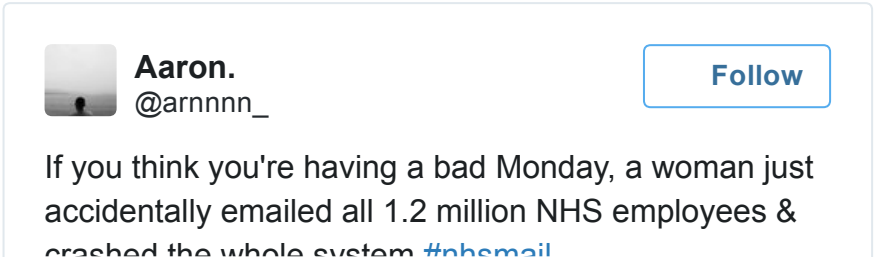
University of Northampton Follow
Welcome to the University of Northampton blog! Featuring student & staff opinion, real experiences an...
Nov 16 · 5 min read

Don't hit Reply-All!

Why we need to rethink email #NHSMail

Associate Prof. Dr Mils Hills takes a different view of the NHS all-staff email mistake.

The recent NHS 'reply to all' debacle is a great example of how the vital systems every business and organization relies on can be brought to heel by very basic human error. We all worry—rightly—about the risks of serious cyber attack by criminals or hostile states, but replying to all in email exchanges can in itself be both a major or a minor threat. In Monday's event, *The Register* reported that "actual work emails were delayed by at least three hours at the time of writing, thanks to the huge volumes of traffic snarling up NHS.net servers".



So, important business correspondence was delayed (maybe lost) by an incredibly simple event.

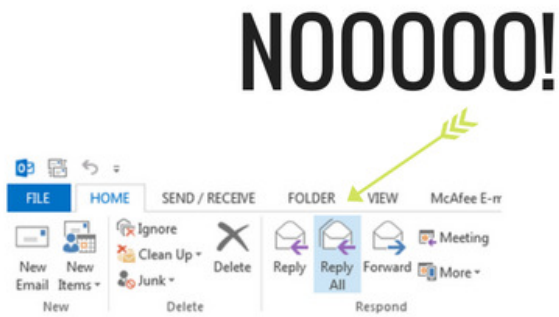
The NHS became even more inefficient and, in addition, because when email systems become overloaded—bad things happen. Information doesn't get exchanged when it ought and sometimes, the confidentiality of systems can be compromised. Add into that the problem of human error—and we have a major problem because:

1. **I'm a member of a Newsgroup where health professionals post compromising information on missed targets and management efforts to avoid missing them, with the full contact details of the poster of the message included.**

2. **I belong to another newsgroup where universities post opportunities for us lecturers to apply for posts as external examiners with them. Several times a week, individuals 'reply to all' to such opportunities with their CV attached …. Providing their personal details amongst other nuggets that could be of value to, say, a criminal.**

What can be done?

It's almost certain that if we work in an organization employing more than a handful of people, we will suffer the pain of working with individuals who hit 'send' to distribution lists or 'reply to all' on messages from such lists. There's no way that technology alone can prevent this challenge—so what can be done?



The key change is *cultural*. Why is it that so few people in public and private sector organisations ask themselves the question **'does everyone *really* need to know this?'** as they consider sending their thoughts on a discussion or document to all. In other words, it's a matter of etiquette. And the growing of awareness that the use of email as a broadcast medium has costs—there is the cost of the employee

writing, the system processing and sending messages, of the recipients reading them, of slowing systems should the attachment or distribution list be large enough.

But beyond that, the cost of missed opportunities—the distraction, stress or anger caused by being thoughtlessly involved in exchanges that can also all to readily escalate into personal diatribe. It is impossible to calculate the loss of value to the organization from thoughts that don't progress because—just as one was about to commit them to paper, screen or memory—the dread email arrived.

> *Why is it that so few people in public and private sector organisations ask themselves the question 'does everyone really need to know this?'*

I recommend that organisations think about email in general in a completely new way. I really like analogies as a way of exploring novel ways of looking at an issue and building toward a solution. At the moment, I'm developing a number of concepts to help organisations increase their effectiveness of their risk and security management processes by using the analogy of the organization having an immune system. Immune systems help animals resist infection—they use a range of processes to tackle invaders from outside—in the form of bacteria, viruses and parasites, as well as defend against problems which are generated within the system. The real power of the analogy will arise from me being able to effectively find parallels between (a) the elements and processes that make up the immune system and the threats to it and (b) the parts of and risks around and within a modern organization. But I think one dimension can already help with the current example. Information flow is critical to organisms and

organisations alike. Feedback from sensors helps the creature understand its environment, coordinates movements and underpins decisions. As data flows up and orders down and across a business—so to, it processes this and manages the production of goods or services. But the smooth flow of information via, say, the nervous system of an animal can be disrupted.

We know that being the unwanted recipient of 'reply to all' messages causes us irritation—equally, inflammation in nerves (from any number of causes) blocks the transmission of critical information from the periphery to the brain and leads to an animal becoming significantly less able to function (at best). Treatments—depending on the cause—include drugs to reduce inflammation or remove the causes of it, whatever the cause—planned intervention is needed. The problem with the email is that a vital system to the modern organization is always at risk—from 'reply to call', clicking on phishing / SPAM links, using portable storage devices, or sending proprietary or confidential data to others (accidentally or otherwise). Engineering-in a protective solution (in other words, making the system immune) requires sustained effort to change how people behave. Such immunisations demand planned activity such that the organization reaps the benefit of intelligent operators who help the system avoid it being exposed to risk from within. Achieving a working culture where people consciously consider whether they need to 'reply to all' at all is not easy, but is needed. Examples such as the unhappy one of the NHS this week could serve as learning opportunities—much like exposing ourselves to attenuated versions of a real disease such that we develop immunity to the full-blown variant. We have seen what could happen —and we actively decide to chart a different course.

This, in short, is the intelligent end of cyber-security: working to produce a socio-technical system which protects itself from the inside-out.

Dr Mils Hills *is Associate Professor of Risk, Resilience and Corporate Security in the Centre for Excellence in Logistics and Supply-chain (CELAS), Faculty of Business and Law, University of Northampton. Prior to joining the University, he has variously been a consultant to national strategic level in the UK, headed research centres in the civil service and was the UK's first 'security anthropologist' for the Ministry of Defence.*

Visit our website information on our courses and find us on social media!