Keeping your business safe from the latest email threats

The SMS guide to spam, ransomware and other online dangers

Contents Page

Introduction

May 1st, 1978 is a day remembered in infamy. This is when the first spam email was sent. Hundreds of people logged onto Arpanet (an early Internet prototype) to find a new message in their email inbox from Gary Thuerk reading:

> WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:
> TUESDAY, MAY 9, 1978 - 2 PM
> HYATT HOUSE (NEAR THE L.A. AIRPORT)
> LOS ANGELES, CA
> THURSDAY, MAY 11, 1978 - 2 PM
> DUNFEY'S ROYAL COACH
> SAN MATEO, CA
> (4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)
> A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

And so began the technological arms race between those sending unwanted emails and those receiving them.

Over time, apps and server filters have worked hard to identify spam and prevent it reaching the recipient. In response senders have used ever more sophisticated ways of pushing messages through firewalls, evading filters, and encouraging unsuspecting recipients to open the email then click a link.

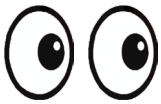
Our white paper on email protection will highlight the latest and most dangerous type of email threats, give you tips on protection, and highlight the business cloud services your organisation can bring online to stop data being infected or stolen.

Before we start, a quick piece of advice. If you are hit by any of the threats outlined here, don't give into the blackmail or extortion and hand over money / bitcoin to the perpetrator. Paying up encourages the sender to keep hitting you for more or passing your details onto others looking to make quick cash.
Instead report the message to the correct authorities. In the UK that's Action Fraud (**https://www.actionfraud.police.uk**) They will advise you on the best course of action.

Threats

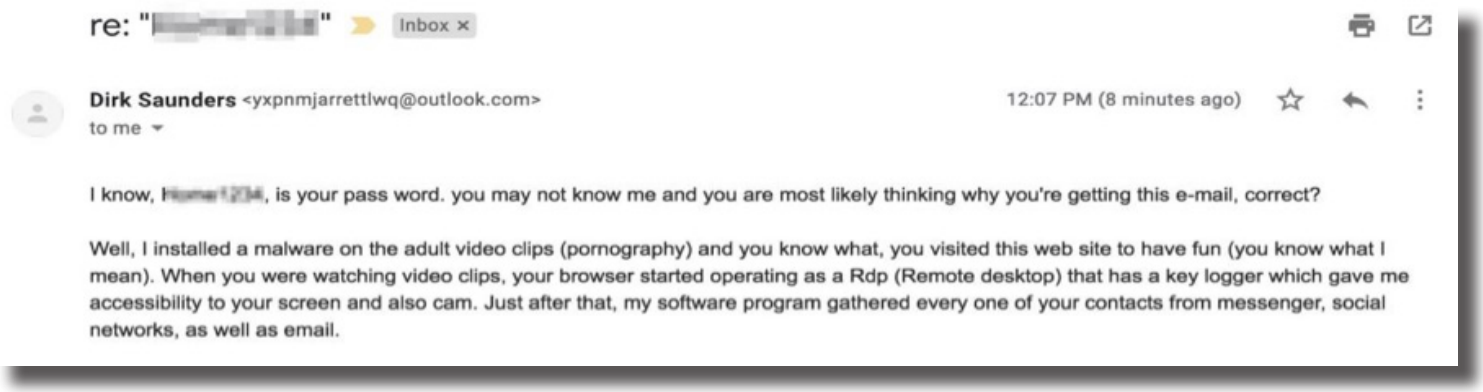
Blackmail! Theft! Bitcoin!

Old-style email spam full of weird characters, random blocks of nonsensical text, clear links, and 'Buye nowe!' messages are nearly always blocked by server-side spam filters and easily identified if they do reach an inbox. The victory against spam has proven to be short-lived though with a new range of more sophisticated and personalised threats emerging.



WE KNOW WHAT YOU DID LAST SUMMER...

There is an increasing trend of extortion emails demanding bitcoin ransoms or your personal browsing history, and other online activity, will be broadcast to family, friends, and employers. What makes these threats appear genuine is they start by telling you your password; **and they're right.**


re: "[redacted]" Inbox ×

Dirk Saunders <yxpnmjarrettlwq@outlook.com> 12:07 PM (8 minutes ago)
to me

I know, [redacted], is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What to do? And how did they get hold of your details?

If your computer is running up-to-date virus and malware protection (either third-party or a built-in service like Windows Defender) then the strong likelihood is that the blackmail attempt is false and the sender has not tracked anything. As for having your password, there's a reason for that...

The truth is, most people use the **same password**, or variant, on multiple on-line accounts, and sometimes companies have their online database hacked and someone downloads a complete list of customer details.

Impact

It's not just small companies either, here are some of the biggest account hacks in recent times:

- Adobe.com **152,445,165 accounts**
- Spambot **711,477,622 accounts**
- Myspace (social networks never truly disappear) **359,420,698 accounts**
- LinkedIn **164,611,595 accounts**

If you had an account on one of these services the email address (and maybe the password) used are available for sale somewhere on the 'dark web'. Which is where the nefarious email sender grabbed your details and sent you a speculative message hoping you'd be startled into paying up.

An email arrives bearing an attachment or, more commonly these days, a link asking you to download an invoice or document. These emails usually appear to come from a supplier, customer, or government agency. They rely on people not carefully checking the email's source and clicking the link or opening the attached file.

And once someone does, a malware file will install onto the PC then start infecting any other suitable machines it can find on your corporate network. The software will sit silently copying itself across the company until ready.

When is it ready? When it has encrypted all your company files and made them impossible to retrieve without paying a ransom. It's too late for a security specialist to do anything about it, and the business grinds to a halt.

It was this kind of ransomware which attacked the UK's National Health Service in May 2017. Disrupting a third of NHS Trust, causing nearly 7,000 operations and appointments to be cancelled.

Awareness

The last threat we'll discuss is a close relation to the previous ransomware; with a cunning twist. It's Friday at 4:45, the office is winding down for the weekend and everyone's attention has turned to their leisure plans.

Then, an email arrives from the CEO, or the Finance Director, authorising a payment. The payee name is recognisable but the bank details are different. Don't worry says the message, they'll explain on Monday but it's imperative the payment goes through NOW. So the stressed accounts clerk makes payment and sends confirmation to the CEO, who responds with:

"What payment? I haven't authorised anything!"

Again, you might think you wouldn't fall this. Remember though the emails look completely genuine with the right company logos, email footer, names, and email addresses. It would take a security expert to know how to spot the fake from a real message.

Protection

Protecting yourself, your business, and your customers

These threats are the biggest growing dangers transmitted via email and every organisation needs to take action to prevent being a victim. Here is the SMS quick step guide to getting safe. The appendix includes relevant links to online resources you should use to learn more about protection and find out what action to take if the worst happens.

Two factor authentication

Start by changing your passwords, ideally by using a password manager, and turn on two- factor authentication for any service that supports it. This will protect you if a current password is being traded on the web and is good, practical, online security advice.

Education, education, education

Start by making sure employees know the danger. Teach them to think twice before clicking any email links, or opening attachments. If you haven't, bring in strict policies about how and when the accounts team make payments and who requests them. Don't allow any payments based on a request from a senior member of staff or director. Insist invoices are required and only suppliers logged onto a CRM system can be paid, and only using the known payment methods.

Boost your spam filters

These new threats need new levels of protection beyond the traditional message scans offered by spam filters. The latest developments in the field of email security are focussed on forensic analysis and email sandboxing to improve threat detection rates and isolate message to prevent network infections.

Keep yourself checked

Find out if you're on any email lists being traded around the web. You won't be able to get off those lists but it will make you more thoughtful about whether to trust incoming emails. Have I Been Pwned? (**https://haveibeenpwned.com**) is a free online checker letting you know if, and how, scammers have gotten your details.

Appendix

To improve email security, SMS offer Advanced Threat Protection:
https://simplymailsolutions.com/products/email-add-ons/spam-filtering

Building on the world-class filtering provided by standard FutureSpam, Advanced Threat Protection adds:

- Sandboxing of incoming emails to test attachments without risking network infection
- URL scanning of links in documents to check the destination is safe
- URL rewriting to invisibly adjust links in emails so they pass through the ATP filter
- Pattern matching to identify email content suspected of being duplicitous
- Authenticity and meta data checks to ensure the integrity of the sender
- Spoofing recognition to identify senders pretending to be other people
- Target detection which identifies attacks on particular individuals

These actions are performed invisibly on every email an organisation receives offering the highest-level of protection available.

Conclusion

The nature of email threats to business has changed. Throughout this guide we've highlighted what the latest and most dangerous threats are, how to get help, and what services are available to protect you from infections in the first place. SMS is an ISO27001:2013 accredited expert in the business cloud and cyber security. Our FutureSpam Advanced Threat Protection is available to customers who host their email with us and those who host email elsewhere, using any modern email platform. To find out more about how we can help get in touch:

Phone: **01925 818448** (UK Business hours)
Email: **sales@simplymailsolutions.com**
Web: **simplymailsolutions.com**

Links

SMS Email filtering and ant-spam services
— **https://simplymailsolutions.com/products/email-add-ons/spam-filtering**
UK Government cyber security advice for SMEs
— **https://www.cyberaware.gov.uk**
UK Cyber Essentials self-help guide and security certification
— **https://www.cyberessentials.ncsc.gov.uk**
Business Advice on spotting CEO fraud emails
— **https://businessadvice.co.uk/tax-and-admin/invoicing/what-is-ceo-fraud-and-how-can-i-identify-it/**
Check if your email is being traded on the dark web
— **https://haveibeenpwned.com**