Praxonomy

Praxonomy e-Book

# Risky Business: THE DARK SIDE OF EMAIL

## Why Email Is More Dangerous Than Ever For Boards

# TABLE OF CONTENTS

# INTRODUCTION

**On August 14, 2019, an unsuspecting professional of Toyota Boshoku, a car components manufacturer member of the Toyota Group, received a vendor invoice requesting payment via email. With sufficient reason to believe it was a valid request, the transfer of funds (USD $37 million in total) was executed. By the time it was discovered that it was fraudulent, it was too late.**

The financial loss was significant enough for Toyota to issue a statement that it would "disclose amendments to its March 2020 earnings forecast documents, if necessary."

This subsidiary fell victim to a BEC (or Business Email Compromise) attack. It's a scam that involves deceiving one or more employees of an organisation with the purpose of having these individuals transfer funds to the criminal's bank account. A common scenario is to hijack a business email account and pretend that the request comes from a trusted business partner — or a high-level executive — to obtain credibility and the victim's trust.

This highly-publicised incident emphasises the need to remain vigilant over email use — even if you don't believe it could possibly happen to you or your organisation.

The adage, "information is power," has been adopted by cybercriminals as gospel truth — and with merit. Time and again, they have used information to manipulate individuals and organisations into adhering to their demands via email.

The good news is that information can serve potential victims of exploits as well: with sufficient user awareness and security education, organisations are able to develop a strong line of defense against email exploits.

That's what this e-book seeks to address.

We want to provide boards of directors and executives with an overarching view of the perilous landscape of email security and present suggestions on how to mitigate the ever-present risks.

More importantly, we want to ensure that the leaders of organisations are able to ask the right questions — so that they can become proactive champions for cybersecurity within, and beyond, the confines of the boardroom.

CHAPTER 1

# WHY IS EMAIL THE "WEAPON OF CHOICE"?

**Despite the emergence of newer communication platforms on the Internet (e.g. social media, messaging, video calls, etc.), email continues to be the most important electronic business communication tool.**

It's not only because emails are considered "official" documents, but also because email works. It saves time and offers tremendous convenience along with ease of use.

Unfortunately, these are the very same reasons that also make it an attractive attack vector for cybercriminals.

Here are some other explanations why email continues to be a sensible first-option for security exploits:

## 1 Inexpensive

Cybercriminals can avail of free email services and platforms to conduct their non-automated attacks. And even if they opt to avail of automated options, the cost is so low that it doesn't discourage them from pursuing scams and cybercrimes. It is possible to avail of a 10,000-node bot for a few hundred dollars.

## 2 User Trust

In 2019, an estimated 3.9 billion individuals were active email users. This number is expected to grow to 4.3 billion users in 2023, which is roughly half the population of the world. To say that email is used widely as a means of communication is an understatement. Criminals capitalise on the fact that it is a trusted, dependable channel for personal and business communication.

### The Widespread Usage of Email

In 2019, global email users amounted to

**3.9 BILLION** USERS

(Statista, 2020)

In 2023, this figure is set to grow to

**4.3 BILLION** USERS

(Statista, 2020)

**That's half of the world's population.**

In addition, email users seem to implicitly trust in the content, links, and attachments sent via emails. Because of the sheer volume of email messages users might receive in one day, users do not spend the time verifying the validity of the information contained in them or the credentials of the sender.

## 3 Flexibility for Attacks

Email scams can be sent out to a mailing list that targets tens of thousands, or it could be sent out to one specific individual. It doesn't limit options for cybercriminals.

## 4 Difficult to Trace

Anyone who has access to the Internet can register for an email mailbox or a domain. In many instances, the net can become too wide to cast to pin down a criminal. It becomes trickier with their ability to execute tactics to evade detection, such as modifying the sender's IP addresses. Tracking and tracing emails can be complicated, tedious, and futile.

## 5 Inherently Vulnerable by Default

Email attackers abuse weak technology and security protocols. For one, the contents of emails, by default, are not encrypted and senders are not typically authenticated.

Most users rely on baseline email security implemented by their providers or vendors, even if secure email usage requires a layered defensive approach. The majority of email users are not privy to this.

As illustrated in the points above, it's easy to understand why hackers resort to email for their criminal efforts.

But how exactly do cybercriminals use email to victimise individuals and organisations of all sizes?

We look at the latest methods employed by hackers and tackle the cybersecurity risks and threats that confront leaders in the next chapter.

CHAPTER 2

# PUT YOUR WALLS UP

**Since email has been around for over fifty years, one might assume that the average user has become acquainted with the modus operandi of cybercriminals.**

This couldn't be further from the truth, and unsuspecting email users are not entirely to blame. The methods and tactics employed by hackers have evolved (and continue to evolve) so much in the last couple of years that even advances in email security technology have struggled to keep up with their pace.

But awareness is key.

The method and intent of attacks may vary, but in many cases, the baseline method of delivery and execution is via email.

In this chapter, we take a look at how email is currently being utilised to attack individuals and both profit and nonprofit entities — as well as how it may simply end up in the wrong hands.

## EMAIL RISKS AND THREATS

### 2.1 Phishing

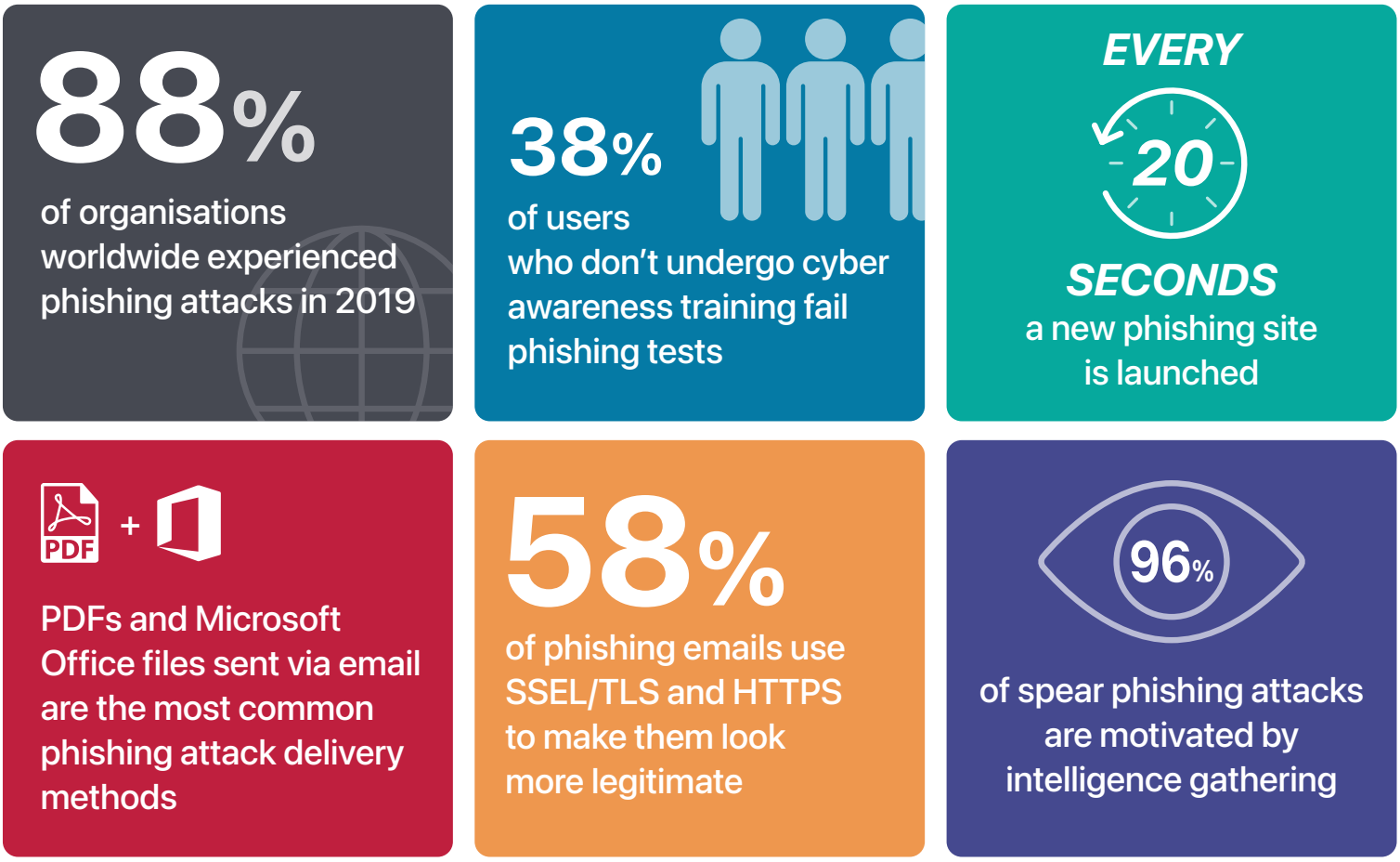
**WHAT IS IT?**

**Phishing** is the attempt to lure a ***collective*** number of individuals into providing sensitive data such as personally identifiable information (PII), banking details, and passwords as required by a hacker posing as a legitimate institution.

The individuals are typically contacted via email, although telephone and text messages are now widely used as well. It is a form of social engineering.

The information obtained is then used to access accounts that can result in data breaches, financial loss, or identity theft.

Verizon's 2020 Data Breach Investigations Report finds that phishing is the top major threat associated with data breaches.




Sources:

https://nordvpn.com/blog/cybersecurity-statistics/
https://enterprise.verizon.com/resources/reports/dbir/
https://docs.broadcom.com/doc/istr-24-2019-en

As it stands, there are at least three other various ways of email phishing. Below are some of them:

## A. SPEAR PHISHING

If phishing campaigns target a number of individuals via mass email, spear phishing attacks hone in on ***specific individuals*** (regardless of whether they belong to an organisation or not). Personalised emails that appear to come from a trusted sender typically infect an individual's devices with malware or are used to obtain PII for theft.

### CASE IN POINT

In June 2020, the Scoular corporation, an Omaha-based commodities trading firm founded 120 years ago, was victimised by an advanced spear phishing wire fraud scam. Cybercriminals targeted a key employee with an email that appeared to come from the CEO. The email had instructions to wire funds to secure the acquisition of a company in China. Believing the request to be legitimate, the employee did as he was instructed. The company lost USD $17.2 million in this scam.

## B. WHALING

Whaling mimics the tactics used in spear phishing, except that the attackers target and conduct research on high ranking victims within a company, from senior management to members of the board of directors.

### CASE IN POINT

In 2015, toy-maker company, Mattel, fell victim to a whaling attack after a top finance executive received an email requesting a money transfer from a fraudster impersonating the new CEO. The company almost lost $3 million as a result.

## C. CLONE PHISHING

Clone phishing requires the hacker to create a replica (or a clone) of a previously received legitimate email to make the victim believe it's real. The email is re-sent from an address that resembles that of the original sender while the body of the email is a clone of the previous message.

The users are tricked into believing that the attachments or links in the new message are the same as the previously received message, but they have been swapped with malicious ones. The attacker often offers a reasoning for the resending of the message. (A common excuse is to state that the contents, i.e. attachments or links, were updated.)

In effect, this attack is based on a previously read, legitimate message which has already gained the trust of the unsuspecting victim.

| PHISHING TYPE | TARGET |
|---|---|
| **Spear** | Specific Individuals |
| **Whale** | High ranking executives / C-Suite / Board of Directors |
| **Clone** | Random and/or Specific Individuals |

# DON'T TAKE THE BAIT: HOW TO IDENTIFY PHISHING EMAILS

- ✔ Be wary if the email is sent from a public email domain (such as gmail.com or yahoo.com, etc.). Most organisations, with the exception of those with small operations, will have their own email domain and company accounts.

- ✔ Take a look at the email address of the sender. Cybercriminals often alter the sender's display name to reflect that of a legitimate organisation, but its email address has little to do with the display name.

  For instance, you might receive a phishing email that may look like the following:

  *From: PayPal <paypal@accts123-reg-02.com>*

  If you'll notice, the display name is legitimate, but the domain, @accts123-reg-02.com, does not reflect Paypal's legitimate domain, which is @paypal.com. The best way to determine an organisation's domain name is to enter the name of the company in a search engine.

  Sometimes hackers simply misspell the fraudulent domain name by one letter, so be careful.

- ✔ Is the email poorly written? Grammatical errors (and not just poor spelling since there's always 'Spell Check') are often good indicators of phishing emails. Hackers do not invest the time to write well-crafted messages nor are they always well versed in the native language of the victims.

- ✔ Is the tone and messaging consistent with the tone of previously received messages from the person/organisation? When in doubt, double check its validity by contacting the sender through an avenue other than email, such as via phone.

- ✔ Is there a sense of urgency to the email? Exclamation points, capitalised letters, and requests to perform an action within a specified deadline or timeframe are typically contained in phishing emails.

- ✔ Are there links or attachments in the email? Unless you are confident that it is from a legitimate party, do not open or click on them. PDFs, ZIPs, Word and Excel files are often used to infect devices with trojans, macros, keyloggers, ransomware, etc. As for links, hover your mouse over the URL displayed. If they are not one and the same, you are likely being redirected to a fraudulent site.

Sources:

https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

https://stealthmail.com/education/the-art-of-email-security

**FYI:** In 2020, cybercriminals were quick to capitalise on the fear and confusion around the COVID-19 pandemic. Phishing emails began hitting inboxes of users to "harvest" their personal credentials. These attacks were so rampant that it prompted the World Health Organisation to issue a statement to warn the public.

Here are some of the compelling phishing Subject Line examples:

- ☑ COVID-19 in your area? Please confirm your address
- ☑ Click here for COVID-19 vaccinations
- ☑ Get your COVID-19 CARES Act relief check here
- ☑ Counterfeit Respirators, sanitizers, PPE
- ☑ Message from the World Health Organization
- ☑ Message from the Centers for Disease Control and Prevention
- ☑ Donate to these charitable organizations.
- ☑ Message from Local hospital - Need patient data for COVID-19 testing
- ☑ COVID 19 Preparation Guidance
- ☑ 2019-nCoV: Coronavirus outbreak in your city (Emergency)

Source: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

## 2.2 Business Email Compromise (BEC)

### WHAT IS IT?

**Business Email Compromise (BEC) or Email Account Compromise** is a cybercrime where a spear phishing email is sent to a key person in an organisation with the intent to make him/her perform an action (such as the wiring of funds) for the financial benefit of the criminals. The emails are made to appear or originate from a credible source.

### CASE IN POINT

Similar to the Toyota Boshoku incident, Japanese media giant and owner of London's The Financial Times, Nikkei, was a victim of a BEC scam as well.

In September 2019, an employee of its US subsidiary, Nikkei America, transferred USD $29 million based on instructions from a high-ranking executive at its parent company. It was a fraudulent email. (Some reports have indicated that the account of the executive was actually "hijacked.") The company is trying to recover the funds with the help of authorities.

# THE FBI ILLUSTRATES THE CRIME VIA THIS TIMELINE:

**STEP 1**
**Identify a Target**

Organised crime groups target companies by exploiting the information available online to develop a profile on the company and its executives

**STEP 2**
**Grooming**

Spear phishing emails target company officials (typically those in the finance department)

May occur over a few days or weeks

**STEP 3**
**Exchange of Information**

The victim is convinced they're conducting a legitimate business transaction

They are then provided wiring instructions

**STEP 4**
**Wire Transfer**

Upon transfer, the funds are directed to a bank account controlled by the organised crime group

The FBI further warns that scammers sometimes have a slightly varied email address that fool victims into thinking the address is legitimate. They then send spear phishing emails to obtain information to execute the BEC scheme.

In many cases, malicious software is involved. These are commonly used to infiltrate the company's network to gain access to legitimate email threads about billing and invoices. These are then utilised to solicit requests (with the right timing) so that it doesn't alarm or raise red flags for accountants or financial officers.

## 2.3 Malware

**WHAT IS IT?**

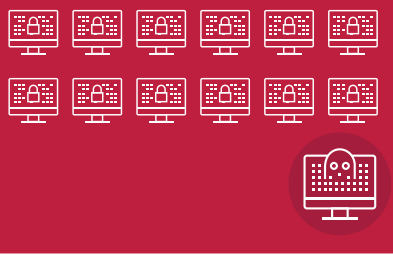
**Malware** is a catch-all term to refer to viruses, trojans, worms, and other harmful computer programs designed to cause havoc in order to gain sensitive information.

**94%**
of malware is delivered via email

**$2.6 million**
is the average cost of a malware attack for a company, making it the most expensive cybercrime

**The cost involves:**
- business disruption
- information loss
- revenue loss, and
- equipment damage

**1 in 13 web requests lead to malware**



**350,000**
new malicious programs and potentially unwanted applications are discovered every day

Sources:

https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/
https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
https://nordvpn.com/blog/cybersecurity-statistics/
https://www.govtech.com/security/Phishing-Malware-Ransomware-Among-Top-Public-Sector-Threats-Reports-Find.html
https://www.av-test.org/en/statistics/malware/

## CASE IN POINT

***Here are two high-profile malware attacks that were executed via email:***

### ILOVEYOU

ILOVEYOU was a worm that spread like wildfire via email in 2000, resulting in more than USD $15 billion in damage. It infected over 10 million personal Windows computers when it started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". Leading individuals to believe it was a simple text file, opening the attachment instead activated a Visual Basic script that damaged the local machine and overwrote files — while sending a copy of itself to all addresses in the address book used by Microsoft Outlook.

This prompted institutions like The Pentagon, CIA, the British Parliament and to completely shut down their mail systems so as not to be infected by the virus.

### Zeus, Zbot, or ZeuS

Zeus is a trojan horse type of malware distributed via email that is used to steal banking information. The malware recognises when the user is on a banking website and records the keystrokes used to log in.

It was first identified in July 2007, when it was used to steal information from the United States Department of Transformation. It became more widespread in June 2009. A security company called Prevx discovered that Zeus had infected over 74,000 FTP accounts on websites of companies such as Bank of America, NASA, Cisco, and Amazon.

## 2.4 Ransomware

### WHAT IS IT?

Ransomware is a form of malware that encrypts files. A ransom is then demanded from the victim in order to restore access to the data. The ransom ranges from a few hundred dollars to thousands, with payments made in Bitcoin.

The most successful types of ransomware are executed in emails with a malicious link or attachment.

### CASE IN POINT

In 2017, organisations in Europe and the US, such as Mondelez International, Merck & Co, Reckitt Benckiser, were crippled by a ransomware attack known as "Petya" — or its variant "NotPetya."

Petya is believed to have spread via phishing that targeted Microsoft-based computer systems.

Petya ransomware was stored in PDF files that came as a package that looked like a job applicant's resume. Once the attachment was opened and permission was granted to make changes to the administrator panel, the system would reboot. It would encrypt the hard drive's file system table which prevented Windows from booting. It demanded urgent payment in Bitcoin to regain access to the system.

There were 188 million ransomware attacks in 2019, and the average cost of the impact on businesses is $233,000. This number isn't expected to dwindle anytime soon.

### 3 POPULAR TYPES OF RANSOMWARE

- **Scareware** - malware that mimics the appearance of antivirus software
- **Doxware** - malware that threats to publish private or confidential information in exchange for a ransom
- **Lockers** - malware that locks users out of their computers

Source:
https://nordvpn.com/blog/cybersecurity-statistics/

## 2.5 Email Spoofing

### WHAT IS IT?

**Spoofing** assumes the identity of a legitimate person or entity to trick users into performing an action. In many cases, it can simply involve spoofing the sender's email display name. This is most common. But sometimes it also includes tactics such as spoofing the entire email address, domain spoofing, and the use of look-alike domains.

Mimecast's State of Email Security Report 2020 (which surveyed 1,025 IT decision makers) reveals that 84% of respondents are concerned about email spoofing. And rightfully so. Spoofing is becoming a popular method for email exploits.

If you've ever received an email where the "From:" field shows your own email or display name, you've likely been spoofed. It may seem harmless, but when you consider hackers could represent you in any or all personal and professional email correspondence (and have recipients believe they actually came from you), it becomes rather terrifying. It's been likened to a form of forgery.

The motive behind email spoofing is deception.

## 2.6 Human Error

### WHAT IS IT?

Email vulnerabilities attributed to **human error** involve the action of accidentally directing emails to unintended recipients.

A December 2020 report from the UK's Information Commissioner's Office (ICO) reveals that misdirected emails have been the top cause for reported data breach incidents in the UK. It has led to 55% more incidents than phishing attacks.

This number is partly due to higher email traffic because of current remote work set-ups. The more emails are sent, the higher the likelihood for error.

Incidents of inadvertently hitting "Reply All" or using an incorrect "autocomplete" entry from one's address book aren't entirely uncommon. But these can have serious consequences — ranging from reputational damage to losing customers due to an erosion of trust. To highlight an example, we bring up Sonos.

### CASE IN POINT

In January 2020, Sonos, maker of wireless audio products and smart speakers, made worldwide headlines when an employee exposed 450 personal email addresses by inadvertently placing all of them in the cc: field instead of the bcc: field of an email. Sonos had to issue an apology. The incident was also reported to ICO. It is now also subject to potential fines.

It is important to note that email addresses are considered PII and are subject to protection under compliance standards like General Data Protection Regulation (GDPR). There can be steep financial repercussions for failure to comply.

## 2.7 Email Bombing

**WHAT IS IT?**

**Email bombing** follows the tactic of DDoS (i.e. "Distributed Denial of Service attacks," where a hacker uses or employs an army of computers called botnet to overwhelm a server — rendering it incapable of processing and functioning.) But instead of targeting a server, email bombing focuses on an email account.

One need not click on a phishing link or download an attachment to be victimised by email bombing. In many instances, the account is simply bombarded with spam to hide or conceal legitimate emails containing important information.

For instance, if your credit card information was stolen by hackers and was subsequently used to purchase a laptop with a transaction record being sent to your email, they might opt to email bomb the account so as to bury or hide the transaction record. It is a method of "covering up tracks" to distract the email owner from detecting fraud or identifying a security breach.

CHAPTER 3

# PLAYING DEFENSE: STRONG EMAIL HYGIENE

**We reiterate this once more: email is not going away anytime soon. And neither are the security threats associated with its use.**

a.) The good news is that the risks are not entirely unmanageable.

b.) In this chapter we offer nine suggestions on how boards of directors— together with the rest of the organisation — can approach email use with practical, prudent information.

## HOW TO MITIGATE THE RISKS ASSOCIATED WITH EMAIL USE

### 1. Use strong passwords and enable Two-Factor Authentication (2FA) whenever possible.

At a minimum, passwords should contain:

- Uppercase and lowercase letters
- Number(s)
- Special symbols (i.e. @%#@, etc.)

Don't use the same passwords across applications. To keep track of passwords, there are a number of password management tools available (such as Nordpass).

Two-Factor Authentication or 2FA adds another defense layer before access to an email inbox can be granted. As the name suggests, there are two factors involved:

a.) information you "know" (such as your password, birthday, middle name, school, etc.)

b.) information provided or generated for you (such as a numeric code sent by SMS, or a code generated by authenticator applications).

Both these pieces of information are required for user access.

Note that 2FA differs from Two-Step Authentication or Two-Step Verification. The latter requires you to provide *information you know* in two consecutive steps. It does not use

external generated codes or devices to grant access.

2FA makes password hacking more complicated and is increasingly being adopted as a baseline for email security.

## 2. Email encryption is necessary.

**WHAT IS IT?**

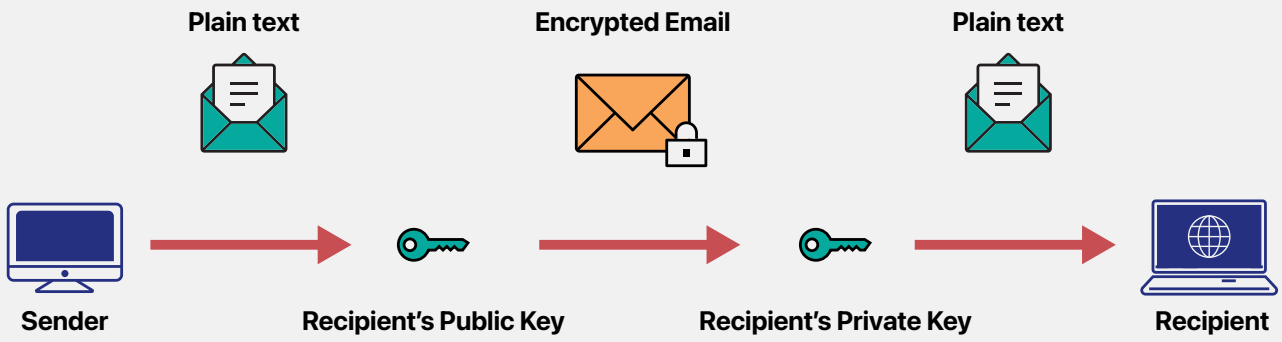
**Email encryption** is the process of encrypting contents of email messages so as to protect sensitive information from being accessed or read by anyone other than the intended recipient.

Emails can be intercepted as they travel over the network. Encryption makes the contents of emails unreadable and uninterpretable "in transit" (as they travel from the sender to the recipient).

Best practice involves encrypting **all** emails you send and receive, so hackers can't distinguish between which emails hold sensitive content versus those that don't. (Be careful about the subject line, these will be sent across the Internet in plain text.)

These days, email encryption functions on the combined use of Private and Public Keys. They encrypt data so that only a verified and legitimate keyholder can successfully access the contents of the message.

Here's an illustration of how it works:




To encrypt email, a Public Key is used to encrypt the message before sending. The person receiving the message must have their own Private Key to view the message. This also establishes you are the legitimate sender via the authentication of your unique Public Key.

These keys are issued by a third-party certification entity. They ensure the authenticity of both keys.

The board should consider utilising secure mail service providers such as Protonmail or Preveil which offer end-to-end email encryption. In other cases, they may need to avail of an email encryption service like GPG Suite, GPG4Win, or Virtru. Virtru allows you to encrypt emails directly from your email client.

It is also important to highlight that email encryption solutions are important for organisations to follow compliance regulations such as GDPR or SOX (Sarbanes-Oxley) or for adherence to security standards like PCI-DSS.

## 3. Implement a Secure Email Gateway.

**WHAT IS IT?**

A **secure email gateway** (or SEG) is technology that iWs designed to prevent the transmission of "bad emails," i.e. emails that break company policy, deliver malware, or transmit information with malicious intent (social engineering, e.g. phishing, BEC, etc.) before they reach a mail server.

With the implementation of a SEG, your organisation can help filter incoming and outgoing email traffic and flag emails with suspicious file attachments, malware, spam, and phishing tactics. SEGs protect organisations from malicious content being delivered to users' inboxes.

SEGs act as a "firewall for email communications." They have features such as virus and malware blocking, spam management, content filtering and email archiving.

## 4. Utilise DMARC (Domain-Based Message Authentication, Reporting, and Conformance).

**WHAT IS IT?**

DMARC is an email validation protocol. It gives email domain owners (such as your organisation) the ability to protect the domain from unauthorized use or email spoofing.

Setting up DMARC alongside a SEG provides a multi-layered defense against email exploits.

Properly configuring DMARC helps receiving mail servers determine how to evaluate messages that claim to be from your domain.

> The primary difference between SEG and DMARC is that a SEG filters the ***contents*** of emails, while DMARC filters the "***From:***" or ***sender*** of emails.

DMARC validation by organisations protect a domain against:

a.) phishing on customers of the organisation

b.) being used in business email compromise attacks

c.) brand abuse and scams

d.) malware and ransom attacks

e.) spear phishing employees and BEC-related attacks

## 5. Be careful with links and email attachments.

All links and attachments should be treated with suspicion.

Most phishing emails contain links or attachments. Links can redirect you to fraudulent sites in order to capture information, and attachments can be used to inject malware into your device(s).

Be especially wary of email attachments containing double extensions or executable files (.exe).

A best practice for sending attachments (to and from board members) with critical information is to use secure file-sharing/share link options that offer end-to-end encryption. One such tool is Tresorit.

These types of tools usually allow files that are shared to have a unique password, an expiration date for file availability, tracking features to see who has opened the file, and file-access revocation. By sending files through this channel, both the recipient and sender receive some assurance that the data they're receiving or sending is secure.

## 6. Back-up data.

In the event that organisations are attacked by ransomware, robust back-ups can save significant time and money.

> Computer Weekly states that best practice for back-ups is the 3-2-1 rule:
>
> Make **three** copies of data, store across **two** different forms of media and keep **one** copy off-site. To protect against ransomware, the offsite backup should be isolated from the business network.
>
> While it is important to back-up files, it is equally crucial to ensure data backup and retention policies are reviewed and tested in order to be reassured that the data can be recovered — or to calculate recovery times.

## 7. Invest in anti-phishing technology.

**WHAT IS IT?**

**Anti-phishing technology** is software that detects phishing content, i.e. links and/or attachments, contained in emails or websites. Once emails are scanned and phishing tactics are detected, they block the content while warning the user that it is fraudulent.

They are often integrated with email clients and web browsers in the form of a toolbar that displays the actual domain name for the website the user is actually viewing. This prevents fraudulent websites from disguising itself as a legitimate website.

The adoption and installation of anti-phishing software is slowly becoming a standard practice, much in the same way anti-virus software is.

There are anti-phishing technologies that can now detect BEC and account takeover attacks.

These solutions utilise artificial intelligence (AI), including machine learning, to create a "baseline pattern for communication patterns and conversation style and detect anomalies in these patterns."

## 8. Conduct regular security awareness training.

An employee clicking on one malicious link in an email has the potential to impact and disrupt business continuity. Employees need to be effective in providing a line of defense for the organisation.

Solely relying on technical security protocols isn't the answer. The reality is that cybercriminals eventually catch up with, or overtake, the advances in cybersecurity and exploit the overreliance of individuals on security technologies.

Security awareness training is key, so is consistent reinforcement. Security awareness programs require an ongoing investment in training and education but will serve the interests and help manage cyber risks of the company in the long-run.

Security awareness training doesn't exclude boards. As discussed in the previous chapter, they are prime targets for exploits as well. The board, together with the organisation's employees, should be well-versed with email security policies and practices.

# 9. Use of Board Portals

## WHAT IS IT?

A board portal is a secure platform for board administrators and directors to organize and manage meetings, access sensitive materials, communicate with each other, and execute their governance responsibilities in a highly secure environment.

Boards cannot afford to be the weakest link when it comes to securing the organisation. Given the sensitivity of information contained in their emails, veering away from utilising an unsecure communication channel is ideal.

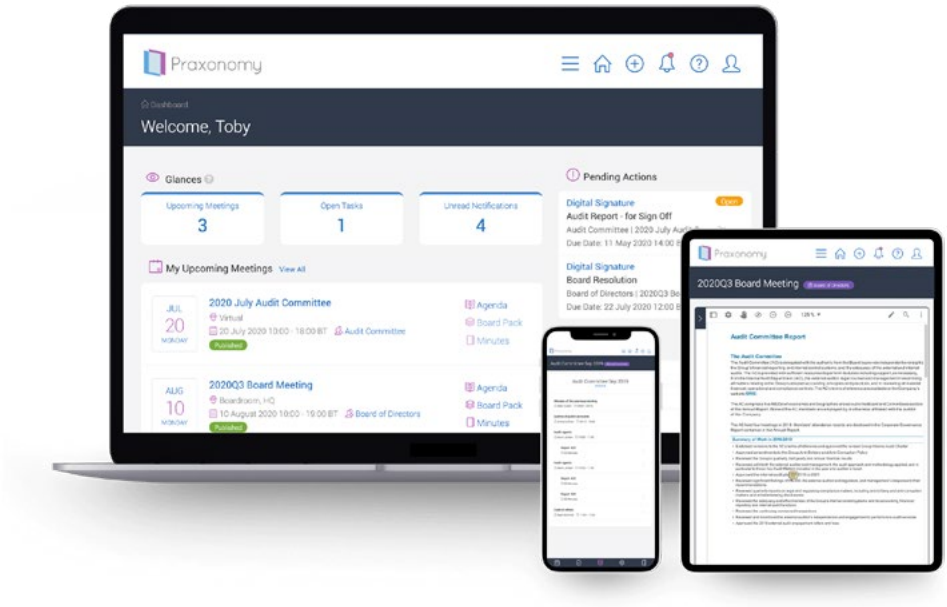
Board portals are an effective alternative to emails for board communications.

Board portals, such as Praxonomy, place significant emphasis on data privacy and security. This covers board-related communications as well.

> Since the use of board portals is limited to authenticated board members or administrators, two risks are significantly minimised - if not eliminated:
>
> 1. That of sending confidential and sensitive information to unintended recipients (misdirected email)
> 2. That of board members falling prey to whale phishing attacks and malware infection

Because board-related communication and collaboration can be done within a highly-secure platform, the need for email as a business communication tool amongst board members diminishes.

Furthermore, data and files stored on board portals are protected by strong encryption, and access rights to individual files can be granted or revoked in real time. This offers boards much greater control over sensitive information than email.



# CONCLUSION

## Emailing will always be risky business.

A healthy degree of caution, mistrust and skepticism has to — and quite unfortunately so — be at play. It is a necessary inconvenience for as long as this medium of communication is employed. The challenge is to understand the thresholds for trusting email, and when that might seep into dangerous territory.

Boards of directors, alongside executives of organisations, will be responsible for setting the tone towards determining this. These times demand that they be advocates for cybersecurity. This whittles down to the use of email and how they present its risks in the context of a wider business narrative.

After all, it no longer is an exaggeration: an ordinary, seemingly mundane email can succeed in bringing an organisation to its knees.

# SOURCES


1. Market Guide for Email Security
2. Number of email users worldwide 2024
3. What happens with unencrypted emails sent over the internet?
4. 2020 Data Breach Investigations Report: Official | Verizon Enterprise Solutions
5. Social engineering explained: How criminals exploit human behavior
6. Must-know cybersecurity statistics & facts
7. Internet Security Threat Report Volume 24 | February 2019
8. Whaling Case Study: Mattel's $3 Million Phishing Adventure |
9. 5 Ways to Detect a Phishing Email: With Examples
10. The Art of Email Security
11. 2020 Phishing and Fraud Report
12. 2019 DBIR Introduction | Verizon Enterprise Solutions
13. The Cost of Cybercrime
14. Phishing, Malware, Ransomware Among Top Public-Sector Threats, Reports Find
15. Malware Statistics & Trends Report | AV-TEST
16. What is malware: Definition, examples, detection and recovery
17. ILOVEYOU and the global pandemic
18. What is Zeus Malware? | Protect Endpoints From The Zeus Trojan Attack
19. Ransomware explained: How it works and how to remove it
20. 34 Shocking Ransomware Statistics (2019)
21. The State of Email Security Report
22. What is PCI Compliance?
23. What is DMARC?
24. Top five ways backups can protect against ransomware