The ProtonMail Guide to IT Security

for Small Businesses

Enforce email security

The ProtonMail IT security team

Enforce email security

READ THIS CHAPTER to understand the email security best practices regarding:

- Phishing attacks
- Imposters spoofing your email
- Email security best practices list

Email security is vital to your business's overall IT security because it is the most common attack vector. Phishing emails and fraud are two attacks that do not require any technical skill, merely an understanding of human nature, a flair for deception, and an email address. Fooling a human into clicking on a malicious link is a much easier way to penetrate a network than trying to hack its firewall.

Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.

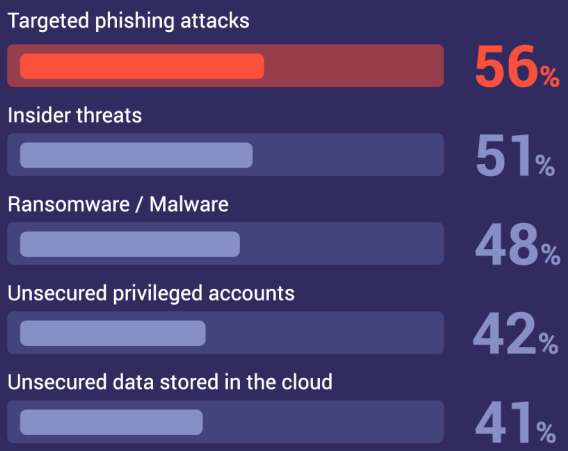
Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.

Receive an email?
DON'T GET PHISHED

Phishing is a type of cyberattack in which a hacker, pretending to be a trusted individual or organization, tricks the victim into opening a malware-containing email.

This can have terrible consequences for your business, including loss of confidential data, leak of financial information and identity theft of your employees' data.

The greatest security threats faced by organization:



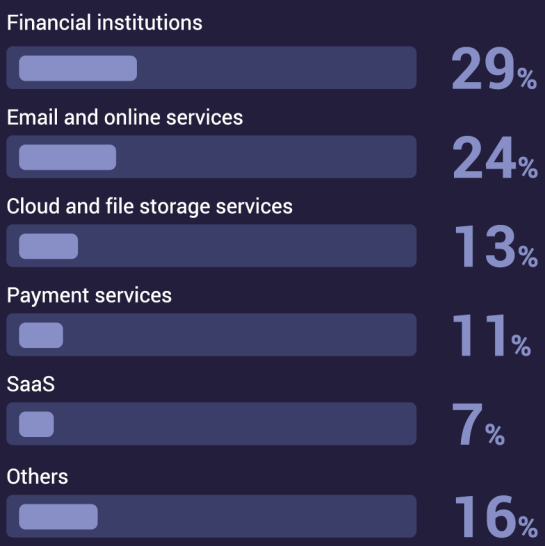
Phishing attacks are the most pressing cyber security challenge

Source:
Cyberark, IT security professional respondents, multiple responses allowed

83% of global infosecurity respondents experienced phishing attacks in 2018

Source: "State of the Phish Report"

Top phishing targets by industry:



Email remains the most popular method of phishing attack

Phishing

Phishing is by far the most common type of IT security threat your business will face. It involves someone posing as a legitimate customer, institution, or colleague to fool your employees into sharing sensitive data, such as business financial details and passwords, or clicking on a malicious link that will compromise their device.

Phishing takes many different forms. Recently, it was reported that Google and Facebook were scammed out of over $120 million by someone who sent forged contracts and invoices asking for payment. Or, in what is probably the most infamous example of phishing, the campaign manager of Hillary Clinton's presidential bid was fooled into clicking on a malicious link and entering his Google password. This exposed his entire Gmail inbox.

Phishing can also involve texts and instant messages, but given email's ubiquity, it is by far the most common medium.

How to prevent phishing

Training

Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. This training should be continuous as well. Phishing attacks are always evolving.

Create a process

Your business will receive phishing emails. So eventually, someone will fall for one. If this happens, your company needs to have a process in place that everyone knows and understands. An employee must know whom to speak with if they think they were just phished. By acting swiftly, you can mitigate the damage of a phishing attack.

Limit public information

Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories, including phone numbers or physical addresses. All these pieces of information can help attackers engineer an attack.

Carefully check emails

First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the "From" address to see if it is odd (e.g., service145@mail.145.com). If an email looks suspicious, employees should report it.

Beware of links and attachments

Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. Attachments are especially dangerous because they may contain malware, such as ransomware or spyware, that can compromise the device or network.

Do not automatically download remote content

Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it.

Never share sensitive information without being sure who is on the other end

No organization should EVER ask for your password via email. If an email is asking you to send your password, credit card number, or other highly sensitive information in an email, this should be a red flag.

Hover over hyperlinks

Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL. You can retrieve the original URL using this tool.

If in doubt, investigate

Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email.

Take preventative measures

Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims

to come from, making it easier to identify potential phishing attacks.

What to do if your company is phished

Follow your company's procedures

Your company must have a process in place for employees who think they may have been fooled by a phishing email. The first step should be reporting the phishing email and any data that was shared to your organization's IT security leader.

Limit the damage

Once your organization understands what the phishing attempt looked like and what information was exposed, your IT security leader should immediately change the compromised passwords. It may also be necessary to disconnect that employee's device from the network to prevent the spread of malware.

Alert others

Your IT security leader should also warn the rest of your employees that there has been a successful phishing attempt and tell them exactly what to look for. Once a phisher sees success with one employee in an organization, they'll often target others to increase their access. You should also inform the company or person that was impersonated that their identity is being used in a phishing scheme.

Notify customers if necessary

If the data exposed affects your clients, make sure you notify the affected parties — they could be at risk of identity theft.

Notify authorities

American businesses should report phishing attacks to the local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to:
spam@uce.gov (an address used by the FTC) and to **reportphishing@apwg.org** (an address used by the Anti-Phishing Working Group).

Imposters spoofing your email

This is when an attacker sets up an email that is identical to your business email address and sends out phishing attacks that appear to originate from your company. This degrades the trust your vendors and customers have in your company.

How to prevent your email from being spoofed

Use email authentication

This type of technology allows a receiving server to verify that an email you sent actually came from your company. This makes it much more difficult for scammers to impersonate organizations.

Domain-based Message Authentication, Reporting, and Conformance, or DMARC, is one of the primary ways to detect spoofed emails. DMARC can also be configured so that you are alerted anytime someone receives an email that appears to be a spoof of your domain.

ProtonMail also has advanced security features, like Authentication Logs, Encrypted Contacts, and Address Verification. Authentication Logs allows you to monitor if anyone else has logged in to your account. If you detect another user on your account, or an active session on a device you don't control, you can remotely log out. Messages sent between ProtonMail accounts are only vulnerable if a hacker compromises the end-user or stages an elaborate man-in-the-middle attack. Encrypted Contacts and Address Verification make it much more difficult for these types of attacks to succeed. These advanced features make it harder for anyone to access, tamper with, or impersonate your emails without your knowledge.

Keep your programs and apps up to date

A hacker could also access your emails through a compromised network. Always keep your security patches up to date and continually update your apps and programs so that you are using the latest version. Ideally, you should set them to update automatically.

What to do if your email is spoofed

Notify customers

If you discover that hackers are spoofing your business's email and using it for phishing attacks, you must tell your customers as soon as possible — by mail, email, or social media. You should inform your customers what your legitimate emails look like, what types of information your company will and will not request, and any other information they can use to spot phishing emails.

Notify authorities

American businesses should report spoofed emails to the local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint.

References

Page 2: 1. Knowbe4, 2018 **2.** FBI, 2017 **3.** PhishLabs, 2019, Phishing Trends & Intelligence Report: The Growing Social Engineering Threat **4.** Symantec, Symantec Internet Security Threat Report-2018, 2018

ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click here.