ATOMICdata

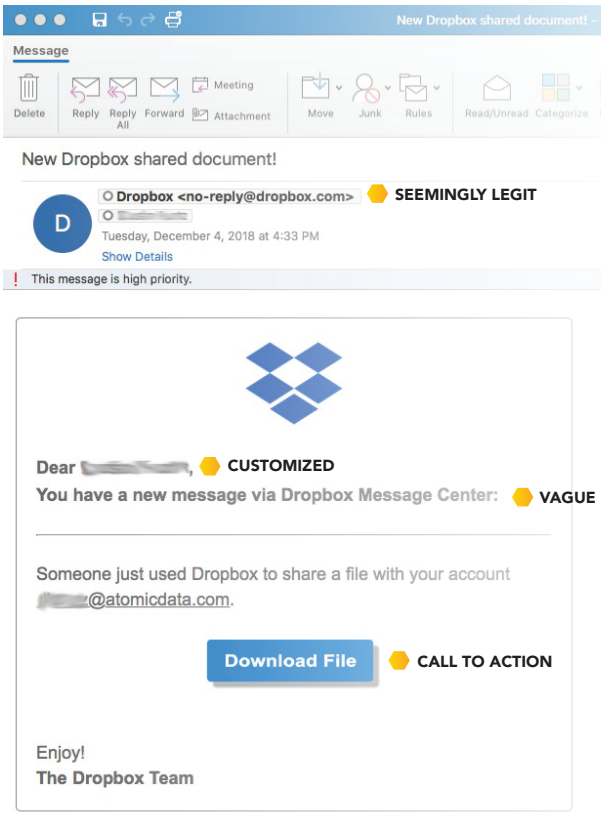
QUICK GUIDE

# PHISHING AWARENESS

**Phishing has become the cyber criminals' go-to attack, especially in times of crisis. Emails designed to obtain sensitive information are getting more sophisticated—making it harder to distinguish what's legitimate and what's not.**

## WHAT IS PHISHING?

It's the act of tricking a person into giving away sensitive information or downloading malicious software onto their PC or company network. It is far easier for criminals to manipulate you to do something than it is to manually hack into your computer or your company network. Phishing is easily carried out over email, it is inexpensive and can be repeated over and over to large lists of recipients.




## COMMON TACTICS

- **SEEMINGLY LEGITIMATE** The first tell that an email is a phishing attempt is a real-ish sender's address.
- **CUSTOMIZED** Often the email is addressed to you in order to seem authentic and gain your attention.
- **VAGUE** The contents of the email are vague but give the illusion of being real by using reference numbers or other information known to you.
- **CALL TO ACTION** The email will include a call to action. It will ask you to log into a website or download a file.
- **FAKE LINKS** The email may feature hyperlinks disguised as legitimate buttons or links. Hovering over the provided link will show the true destination—likely ***not*** the institution's trusted web address. Be on the lookout for slight variations including misspellings and alternate characters (eg: Drop-Box.com instead of Dropbox.com)

**Phishing comes in many forms,** and even the most vigilant users can be fooled. Everyone in a company must stay up-to-date with the most popular social engineering tactics. Below are some key terms and tips for you to stay ahead of any would-be phishers.

## TYPES OF PHISHING

**MASS PHISHING** the most common example of phishing. Emails are made to look like they came from a legitimate source. These are bulk emails that may only address the receiver as "client" or "customer." Attackers will use a sense of urgency or threat to make you act without thinking. W2 emails during tax season and teleconferencing related emails during the COVID-19 pandemic are increasingly common examples.

**SPEAR-PHISHING** Similar to phishing, but these emails target specific people. Using information gathered from social media accounts like LinkedIn, phishers use your personal information to fool you into handing over important information.

**CEO/EXECUTIVE FRAUD** cyber-criminals will pretend to be executives or attorneys in your organization. They will use intimidation to pry info out of employees or initiate fraudulent transfers. This is often attempted when the executive is traveling or out of contact.

**FRAUDULENT TRANSFERS** Hackers will spoof emails from vendors, banks executives, or billing departments asking for a wire transfer or large purchase. This is an increasingly common, highly lucrative method. The attack is often carried out after a period of lurking, where the attacker, already inside your email or network, will silently watch and wait for the right opportunity.

## ANTI-PHISHING TIPS

- **BE SUSPICIOUS** Hover over links before clicking on links embedded in emails. This will show the actual destination of a hyperlink. Also ask yourself, 'Is this an expected email?'.
- **TRUST YOUR GUT** If an email looks "off" or "weird" it probably is. Look for misspellings of common words or names, email addresses that look slightly different, and unnecessary urgency.
- **PLAY IT CLOSE TO THE VEST** Avoid posting personal information online. LinkedIn, Facebook, blogs—take care not to divulge information that could be used for social engineering.

- **CONFIDENTIALITY** Never send confidential information over email (e.g. usernames, passwords, CC numbers).

## HOW TO PROTECT YOUR COMPANY

**IDENTIFY HIGH RISK USERS** like C-suite executives, Attorneys, Accounting and IT administrators. These individuals must remain hyper-aware of cyber-attacks. **IMPLEMENT TECHNICAL CONTROLS** such as two-factor authentication, password policy enforcement, patch management, mail filtering, etc . **WRITE & USE A SECURITY POLICY**, agreed to by all employees. Including: mandatory annual security training, password management, acceptable use, etc. **PLAN FOR BACKUP, DR, & INCIDENT RESPONSE** Regularly scheduled backups and data retention, a disaster recovery policy, and a documented incident response plan must be in place. **TEST PHISHING AWARENESS** through phishing emails sent to employees on a regular basis by an internal or external IT security resource.



ATOMICdata