ATOMICdata

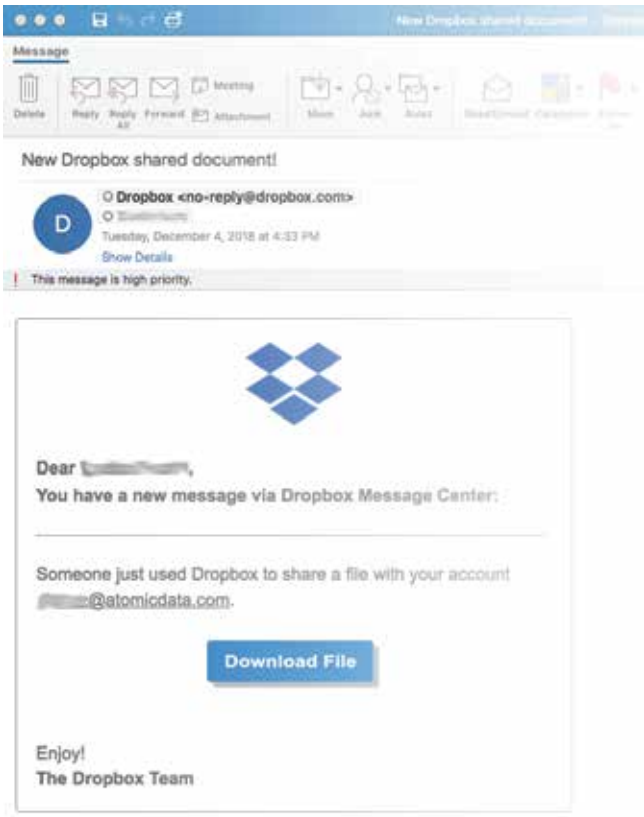
QUICK GUIDE

PHISHING AWARENESS

Phishing has become the cyber criminals' go-to attack. Emails used to obtain sensitive information are getting more sophisticated—making it harder to distinguish what's legitimate and what's not.

PHISHING DEFINED

Phishing is 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. Please see the tips below:



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. This is called "spear-phishing."
- **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.
- **CLICK HERE** 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.

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.

ANTI-PHISHING TIPS

BE SUSPICIOUS Hover over links before clicking on links embedded in emails. This will show the actual destination of a hyperlink.

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)

PHISHING TYPES

PHISHING he 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.

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.

FRAUDULENT INVOICES Hackers will spoof emails from vendors, banks or billing departments asking for a wire transfer.

STILL WORRIED ABOUT FALLING VICTIM TO PHISHING?

Atomic Data can help you prepare for the worst with IT Security as a Service.

- **VULNERABILITY SCANNING**
- **PATCH MANAGEMENT**
- **POLICY ADVISORY & DEVELOPMENT**
- **SECURITY AWARENESS CONSULTING**
- **TWO-FACTOR AUTHENTICATION**
- **PHISHING SIMULATION & EDUCATION**

ATOMICdata