Cybersecurity Best Practices:

Protecting Against Malicious Emails

Given email is such a heavily utilized communication tool, it is frequently targeted for malicious attacks. This is a friendly reminder of what to look out for when handling emails, and what to do when you receive a suspicious email.

Phishing Scams

Email that appears to be from someone in authority, IT, or a trusted business attempting to trick you into revealing information whether it's your password to the network, or your credit card information. This is the most common form of attack.

"Click on this link" e-mails

Deceptive emails trying to trick you into clicking on a harmful link — to compromise your computer, steal information or passwords, or trick you out of money. Even legitimate-looking URLs can lead to malicious web pages.

Attachments

Emails can contain attachments that have malware embedded within it (normally .zip files). Once opened, they'll infect your computer and proceed to attack the rest of the network. You may have heard of Cryptolocker and other ransomware viruses — they are normally sent out using this method.

A good example of this are fake e-card emails that contain attachments-while the body of the message will say it's a funny video attached, it's most likely a malicious attachment.

Generic Spam

Unsolicited bulk email, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers – our Office365 spam filtering system does a good job at catching these messages, but occasionally they can slip through, particularly as bots get more crafty.A good example of this are fake e-card emails that contain attachments-while the body of the message will say it's a funny video attached, it's most likely a malicious attachment.

Privacy

Never assume that email or attachments are private or confidential.

Scam Messages

You've all seen this before- an email promising an insane amount of money as soon as you send your bank account information and social security number. It's not real. It's never real.

Some sure signs of a "scam" email:

- It asks you for a password
- It asks you for personal or financial information, or for money
- It is not addressed to you by name
- It is grammatically incorrect
- It asks you to forward it to lots of other people

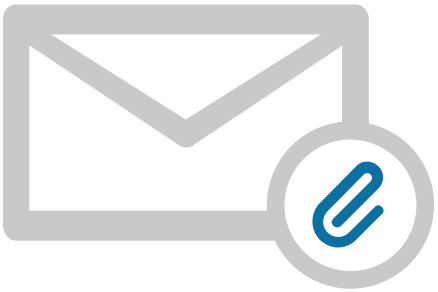
DATAPRISE

Avoiding Malicious Links & Harmful Attachments

Don't click on links in email unless you REALLY know where you're going.

If an email is unsolicited or even slightly suspicious, look up the website yourself and go there on your own instead of clicking on a link in the email. This includes:

- Links in what appear to be bulk emails - especially if they aren't addressed to you by name
- Security alerts - Example: Don't use a "Microsoft software security update" link in unsolicited email.
- Emails telling you to follow a link in order to verify or fix a problem with your account.
- Cryptic or shortened URLs (e.g. Tiny URLs) - these are particularly risky because you can't easily tell where they are supposed to go
- Bargains and "great offers," or links to claim an award/reward
- Links to pictures or videos from people you don't personally know



Don't open email attachments unless you REALLY know what you're opening.

If it looks suspicious, don't open it. Some examples of suspicious messages:

- Not work-related
- The email containing the attachment was not addressed to you, specifically, by name
- Incorrect or suspicious filename
- Unexpected attachments
- Attachments with suspicious or unknown file extensions (e.g.: *.zip, *.exe, *.vbs, *.bin, *.com, *.pif, or *.zzx)
- Unusual topic lines; "Your car?"; "Oh!" ; "Nice Pic!"; "Family Update!"; "Very Funny!"

How should I deal with a suspicious e-mail?

If an email matches any of what was mentioned above- don't open, forward or reply to it, just delete it.

If you receive something that looks to be coming from a legitimate source but still looks suspicious, please contact support@dataprise.com. We will gladly take a look.

DATAPRISE