NEXTWORKS™

Email Security Awareness

Even with antispam technologies, “phishing” scams are at an all-time high. Unfortunately, there is no easy technical solution to this problem. It is the responsibility of all individuals within the organization to ensure they understand how to identify and avoid phishing attempts.

The goal of a phishing scam is simple. The attackers hope to impersonate someone with authority within your organization (often a CEO or Manager) and get you to take actions that result in financial loss or other damages to the organization.

Alternatively, the attackers will send an email impersonating a vendor, such as Microsoft or Google, asking that you confirm your identity, billing information, etc.

These simple steps can help you prevent becoming a victim:

1. Rarely trust email from entities you don’t know. And if you do know them, be alert if their email requests a peculiar action. Maybe it’s not really them, or perhaps their email was hacked.

2. Do not provide sensitive personal information (like usernames and passwords) over email.

3. Verify the *From:* address in an email. And verify links in email. (explained on page 2)

4. Contact the individual making the request and confirm legitimacy. (Don’t just click Reply.)

5. If in doubt, forward suspicion email to support@next-works.com.

Thank you for helping to keep your data, network, and computers safe from these cyber threats.

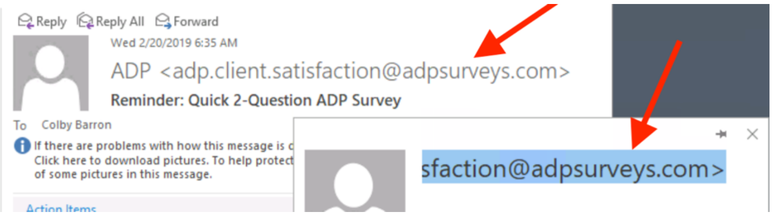
More detailed technical information is on page 3 if interested.

How to Verify the “From” Address in an Email

On the surface, an email may appear to be from someone familiar. If you are in doubt, or something seems out of context, confirm!

Observe the email address (not just the name). Depending on your version of Outlook (or other email client), you can often see the address. Sometimes you need to mouse over the name, or right-click on it.

Here we have an email from ADP. Is it from ADP? Notice the address is adpsurveys.com. This seems legitimate.



Wed 2/20/2019 6:35 AM

ADP <adp.client.satisfaction@adpsurveys.com>

Reminder: Quick 2-Question ADP Survey

To Colby Barron

If there are problems with how this message is d
Click here to download pictures. To help protect
of some pictures in this message.

sfaction@adpsurveys.com>

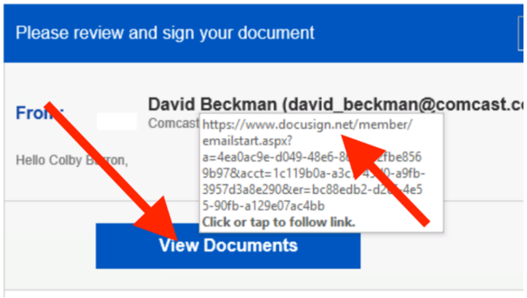
This test doesn’t provide 100% assurance. But it certainly helps.

How to Verify a Web Site Link (URL) in an Email

While is best to avoid clicking links in email in general, it is nearly impossible to get work done without sharing links.

When you must click a link, first verify where the link goes. Here is an example:

You may receive a link that appears from Docusign. But let’s mouse over the link to confirm *where* we will actually go.



Please review and sign your document

From: David Beckman (david_beckman@comcast.c
Comcast

https://www.docusign.net/member/emailstart.aspx?a=4ea0ac9e-d049-48e6-8[illegible]fbe8569b97&acct=1c119b0a-a3c[illegible]-a9fb-3957d3a8e290&er=bc88edb2-d2[illegible]4e55-90fb-a129e07ac4bb
Click or tap to follow link.

Hello Colby Barron,

Notice here that we are going to docusign.net. This is legitimate. (It’s not something like docusign.cx1.ru.)

Q & A

Why doesn’t my spam filter help?

These are personal emails. They are written from one individual to another. They are sent from a legitimate mail provider such as Google, Yahoo, Outlook.com, etc. It’s difficult for a spam filter to detect them all. Many get blocked. Some don’t.

What if emails are going out to people *from* me that I didn’t send?

See our other whitepaper, “Email Spoofing”.

Types of spam emails:

Scams: Intentional deceptions made for gain, or to cause damage through email. For example: “You are a winner of our £1,000,000 lottery fund! Click here to claim your reward.”

Spam: Also known as junk email, designed to trick you into thinking their message is worth reading. For example: "Great value medical store!"

Hoax: Warnings about a non-existent threat, or an offer that sounds good to be true. For example: "Your Dropbox account will be deactivated in 24 hours unless you confirm your email address and password."

Phishing: Pronounced ‘fishing’. Phishing emails try to entice you into disclosing personal information, such as your username, password or bank account details. For example: "You have been given a tax refund. To help us process your payment, please click here and enter your name, address, phone number and bank details."

Many phishing/scams emails contain spoofed email addresses and link in the body:

Spoofing: When the sender address of an email has been altered to hide its true origin, used by virus and spam authors to make their emails look legitimate and lure people into clicking on links or downloading attachments. For example: The email looks as it is from one address but hovering over it reveals a different address.

The most worrisome emails are the targeted phishing emails, which at first glance can seem very real/genuine. We’ve outlined a few different types of phishing attacks to watch out for:

Phishing: In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.

Spear Phishing: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to your company name in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.

Whaling: Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to yours, they look like normal emails from a high-level official of the company, typically the CEO or CFO, and ask you for sensitive information (including usernames and passwords).

Shared Document Phishing: You may receive an e-mail that appears to come from file-sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.

Several aspects of phishing emails that are especially concerning:

Doppelganger: Utilizes fake e-mail domains that look similar to your domain.

A hurried tone: They will often ask you to send money immediately, stating that they’re busy or in a meeting, and can’t do it themselves.

E-mail only: Since these types of emails rely on impersonating an employee via a fake, yet similar email address, they will ask you not to call with questions and only reply through e-mail.