Security Training and Best Practices

- What to do if you get a phishing email or smishing text
- Email Security here at eFileCabinet (Proofpoint vs Barracuda)
- Managing your Barracuda Quarantined Emails
- Three Things to look for in Phishing Emails - Phishing Training

What to do if you get a phishing email or smishing text

What is a phishing email?

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, phishing is by far the most common attack performed by cybercriminals, the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.

What to do if you suspect an email you received is a phishing email

If you are confident that you have received a phishing email, please forward your email to security+phishing@efilecabinet.com - You don't need to do anything else. We will log the email and use the data to help improve our email security.

What to do if you are unsure if an email is phishing or legitimate

If you are unsure if an email you receive is phishing or legitimate please still forward your email to security+phishing@efilecabinet.com but also include a note with the email stating that you would like it to be evaluated. The security team will evaluate the email and let you know if it is safe or not.

What are we doing here at eFileCabinet to combat phishing?

We employ a professional service for email security. Despite this, phishing will always be persistent and will continue to get more sophisticated. The best thing we can do to combat phishing is to educate ourselves. You should have already taken a phishing course. Additional, we conduct a yearly phishing campaign where we intentionally email (non-malicious) phishing emails to employees to ensure that employees are following correct protocols when receiving phishing emails.

What about smishing?

Smishing is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers. Smishing is implemented through text messages or SMS, giving the attack the name “SMiShing.”

Because you receive smishing texts on your personal device, there is little we can do to help employees combat smishing. Please use common sense and your best judgement when receiving a suspicious text. You are welcome to report incidents at security+phishing@efilecabinet.com

Email Security here at eFileCabinet (Proofpoint vs Barracuda)

In order ensure optimal security practices here at eFileCabinet, we use third party software to help protect employees from receiving phishing email, spam, and malware in their email.

For the year 2022, we have been using Proofpoint.

We are currently evaluating the switch to Barracuda for email protection. Among other things, Barracuda can provide us with

- Spam and Malware Protection
- Attachment and Link Protection
- Email Encryption and Data Loss Prevention
- AI-based detection of social engineering
- Automatic Remediation

Why are we making the switch from Proofpoint to Barracuda?

From an end user perspective, the only way to train Proofpoint is through the daily quarantine emails. Unfortunately the format for these emails can be confusing. Furthermore, the quarantine emails show emails for the entire month. Because each email digest has so much redundancy, people tend to ignore these emails rather than using them for how they should (namely, improving the allow and block list).

Barracuda has a much cleaner format for the quarantine emails with useful descriptions for the actions you can take for each quarantined email (Deliver, Allow, Block). Barracuda only shows each quarantined email once.

Examples of Differences

Below you can see a small portion of my daily quarantine email from Proofpoint. It shows all quarantined emails from the last 30 days. Because of how long this email is, most employees simply start ignoring this email and potentially miss quarantined emails that should be allowed through.

2022-11-14_15-31-46.png
Image not found or type unknown

Below is the quarantined email digest from Barracuda. It only shows the new quarantined emails in the digest so it will never be a long list. Each email has links you can press to deliver, allow, or block. If you regularly block and allow emails you will start to get fewer quarantine emails.

2022-11-14_15-08-33.png
Image not found or type unknown

What you need to do

Nothing. You do not need to make any changes on your end. Suspicious emails will be quarantined just as they have always been, there will just be a new service (Barracuda) doing this. If you would like to improve the emails that are being quarantined, you can open your digest of quarantined emails and click on "allow" or "block".

If you suspect that a valid email message was blocked, please contact IT and report the details so that we can change the filtering rules to make sure all valid emails get through to you.

Managing your Barracuda Quarantined Emails

You can manage your own Barracuda settings and block or allow quarantined messages. To do this please follow the instructions below:

- Find an email from Barracuda about quarantined email (search for "Defense Quarantine") and click on the link that says "Manage Quarantine". Or go directly to

  https://ess.barracudanetworks.com/user/auth/login

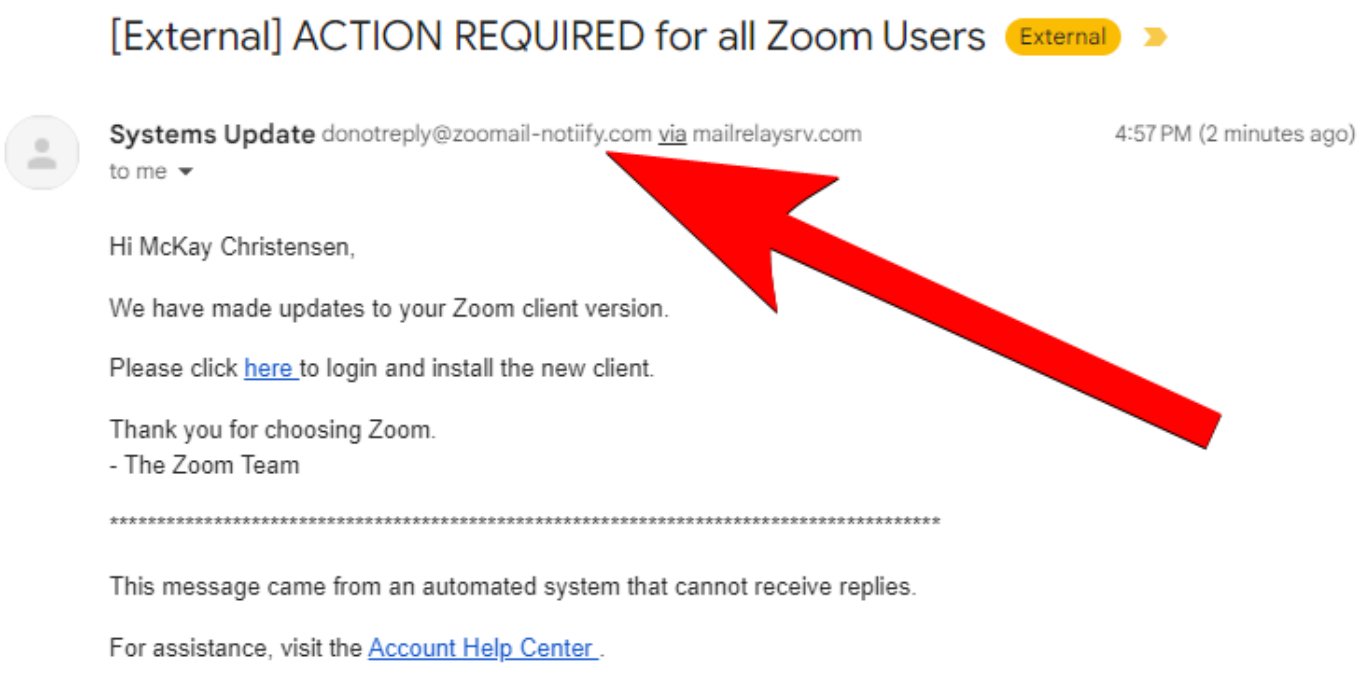
  - image.png Image not found or type unknown
- Enter your email address then click "Next"
  - image.png Image not found or type unknown
- If you have already set a password, you can enter it now. If you never set a password of have forgotten what it is, please lick on the "Send login information" link.
  - image.png Image not found or type unknown
- Check your email and click on the link that was sent to set up a password
  - image.png Image not found or type unknown
- You can now go through your message log and block or allow messages
  - image.png Image not found or type unknown
- Or you can change how often you get email notifications
  - image.png Image not found or type unknown

Three Things to look for in Phishing Emails - Phishing Training

Phishing emails can be hard to spot. Here are three things you should check before you click on a link in your email:

Check the sender email address.

Look at the email address. It it does not make sense, has typos, or seems suspicious then ignore the email or forward it to phishing+security@revverdocs.com



Check the body of the email. Are you expecting an email like this?

If the email seems out of place or does not seem completely logical, there is a good chance it is a phishing email.

Hi McKay Christensen,

We have made updates to your Zoom client version.

Please click here to login and install the new client.

Thank you for choosing Zoom.
- The Zoom Team

****

This message came from an automated system that cannot receive replies.

For assistance, visit the Account Help Center .

Hover over the link before clicking on it.

When you hover your mouse cursor over a link, it will say what the URL is. If the URL looks suspicious, then don't click on it. **IMPORTANT NOTE**: We use Barracuda for our email security; Barracuda takes extra security measures to protect links. If you see a link that starts with https://linkprotect... then the link is from Barracuda. If you click on it and it is a valid link, Barracuda will redirect you. If the link is malicious, Barracuda will not allow you to open the link.