

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](#). Additionally, 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

Revision #3

Created 5 October 2022 21:00:06 by McKay Christensen

Updated 6 October 2022 23:07:56 by McKay Christensen