What are Malicious Attachments? Transcript

Malicious Attachments

Meet Lily. She works for a large corporate organisation.

Lily has had a great week, however, she still is glad that it's finally Friday. Working in HR is tough and trawling through CVs on a daily basis can be monotonous work.

Thankfully Lily has had a productive Friday morning and she has compiled a list of possible candidates for several of their job vacancies. Lily decides she will finish reading the last few emails and treat herself to a well-deserved coffee break.

Lily is often appalled at the spelling that she receives in many cover letters. Can no one spell anymore? Is grammar a thing of the past?

Due to this, Lily ignores the bad grammar and opens up the second last email containing a CV attachment. Before long Lily realises that the CV is unlike any she has received before. This candidate seemed to have potential, but maybe not for the job that Lily had advertised.

The attachment was not a CV. It was actually malware. Very quickly Lily realises that something has gone very wrong. Her files have been encrypted and her computer is now displaying a ransom note demanding that she pay to get her files back.

Lily doesn’t feel like treating herself to that morning coffee anymore.

Email users regularly receive unsolicited emails from unknown senders. These emails can often contain links to malicious websites or have attachments containing malicious software. This can be used to destroy data and steal information.

A popular scam is to send an attachment containing malware disguised as a CV or cover letter. The HR department is a perfect target for a cybercriminal as they receive multiple CVs from unknown senders on a regular basis and therefore would not be alarmed by receiving one of these emails.

The danger is that some malware attachments can give the attacker control of the user’s device, access to their screen, capture keystrokes and allow access to other network systems.

It is always best practice to hover over any links embedded within emails, be wary of any attachment that isn’t a .txt file.

And remember you are the first line of defence against cybercriminals.