Reporting Phishing Emails and Why It's Important

[music playing – all the animations appear on a computer monitor]

Text on screen: Val's catching up on her emails.

[There's an email programme open with three new emails]

[Val's thoughts appear in a bubble]

Julie's happy with that. Next

[An email asking her to a catch-up meeting.]

Thought bubble: I can't do Monday morning. I'd better let Blake (the sender) know.

[She writes an email suggesting a later time and sends it.

The last email appears on screen. It says that someone has tried to logon to her account from an unknown computer and that it if wasn't her, she should confirm by logging in – a link to login is provided.]

Thought bubble: Someone's tried to log on as me. It wasn't me. Yes I can confirm.

[Val follows the link to the login page and logs on with her username and password.]

[A thank you message appears on screen]

Thank You
Your credentials have been confirmed
We appreciate your help
IT Support Team

Subtitle: Perhaps it should say.

We can now log into your network

Send emails from your account
Access the same files as you

Subtitle: Cyber criminals can now access the network as if they were Val. So what happens next? Probably nothing visible to Val. Like burglars hackers rarely let you know when they've broken in.

[We see the phishing email again]

Subtitle: It's a shame Val didn't spot the spoofed email address.
[zooms in to the email addresses and highlights that one letter is different in the address]

Subtitle: To be fair, it's really hard to see

[highlights the request for username and password]

Subtitle: A confirmation like this should be Yes/No not a username and password, which perhaps should have raised suspicions. However, at the point the worst thing to do is nothing.

Text on screen: The worst thing to do is nothing.

Subtitle: If you've responded to a phishing email by mistake, you should report it as soon as you can.

Text on screen: Report it. Help stop the attack. Protect Others.

Subtitle: Who you report it to will depend on your situation and the type of email. Here are some suggestions.

Text on screen:
IT Team/Support
If you work for an organisation that has one, this should be your first call. Make sure you contact the genuine team.

You can search report phishing scam plus the name of the email/message provider.

When criminals pretend to be from an organisation, search report phishing scam plus the name of the organisation.

National crime agencies want to track phishing scams. Search report phishing scam plus the name of the country you're in.

[music fades]