Spam and Phishing at Charles Darwin University

Transcript

0:00 Welcome to this presentation on Spam and Phishing at Charles Darwin University.
0:05 In this presentation, we will be talking about what spam and phishing emails are.
0:10 The scale of the problem.
0:11 The consequences of replying to those emails
0:15 What ITMS does about spam and phishing
0:17 How to recognise them and
0:18 How you can help us.
0:20 So, what is spam and phishing?
0:23 Spam are emails that sent to a recipient that are not wanted, similar to the junk mail you would get in your home letterbox.
0:32 and phishing are emails asking for your username and password or with links to websites that ask you to login with your username and password.
0:41 So how big is the problem?
0:44 CDU receives a large volume of emails every day and a big percentage of those are spam and phishing emails.
0:52 It is estimated that 60% of global emails are spam and phishing.
0:58 Spam and phishing emails are a global problem.
1:01 A problem faced by all large organisations.
1:04 A risk to an organisations status and reputation.
1:08 A waste of an organisations resources and are
1:11 Just plain annoying.
1:13 So what happens when an account is compromised?
1:16 A compromised CDU account starts to send out emails, spam.
1:20 Compromised means it has been taken over they've got you username and password and they've started using it for themselves.
1:28 The keepers of the blacklists, identify these emails as coming from CDU.
1:34 CDU is added to the blacklists. This results in all emails from CDU being blocked not just those of the account the emails are being sent from but all of them. Being on a blacklist is a bad thing.
1:49 Other organisations and government departments subscribe to these same black lists and also block all CDU emails.
1:57 Emails from CDU are either bounced or rejected by those additional organisations.
2:02 And everyone at CDU is unhappy because their emails aren't getting through and the people they want to talk they're not getting those emails.
2:11 So what are the consequences?
2:14 All CDU staff are inconvenienced.
2:18 Emails from staff and students are being delayed.
2:22 ITMS has to spend time and effort getting CDU off those blacklists and

2:28 the reputation of CDU is placed at risk, as we start to get a reputation as being an origin of spam.
2:36 So what does ITMS do about it?
2:38 We scan all emails coming into CDU for spam, viruses and Trojans.
2:45 We use graylisting, this is where a suspect email is initially blocked, which stops spam emails, but legitimate email retry and are allowed through on their second attempt.
2:57 We subscribe to those same blacklists that we're trying to stay off of and
3:03 when identified we manually block emails that manage to get through all of the above.
3:08 We educate staff not to give out usernames and passwords so those accounts are not compromised in the first place.
3:16 If we see any large emails being sent out we flag those accounts and we check them to make sure they are actually legitimate.
3:24 So why can't ITMS block all spam?
3:26 The process is automated and the filtering employed is not 100% dependable.
3:31 If the filtering were stricter, legitimate emails would be blocked and then we would be having complaints from people that their email weren't getting through.
3:39 Spammers adapt to how the filters operate and learn how to beat them, so it's a bit of a competition between the spammers and the people that make up the filters.
3:49 And the filters need time to be updated. We get the filters from the people that maintain them and it takes a little bit of time for us to put them into place.
3:59 So how can I recognise spam?
4:02 Ask yourself "Am I expecting this email?"
4:06 Check the senders email address. Do you recognise it? It is something you've seen before.
4:12 Does the language of the email have a lot of spelling and grammatical mistakes? A lot of the people sending out spam are quite amateurish and the emails show it.
4:22 Is it believable? A lot of email aren't very believable.
4:28 Does the email have links going to non-"cdu.edu.au" addresses?
4:34 Here's an example of a phishing email. In the From it says it's from Charles Darwin University, but let's have a closer look.
4:43 The email address. It doesn't end in cdu.edu.au it ends in webmail.cbu.caj
4:50 And it's calling something the Admin Help Desk. Never heard it called that before.
4:56 And we have a link here, let's put our mouse over it, but weren't not going to click and see where this might take us?
5:06 Okay it wants to take us to grandvisionbg.com/1/kicks.htm.
5:14 Why do I need to go here? It doesn't have cdu.edu.au at the end of it.
5:18 Let's look at another example of a phishing email.
5:22 Let's look at the address. Again it's a funny email address and we've got a web link here.
5:30 Now this one has cdu-mailcdu.edu.au. Now this is being a bit tricky because it trying to put a legitimate one there into the link,
5:38 but if you have a look at the end of it, it doesn't end in cdu.edu.au it ends in webs.com.
5:44 And it's calling it the ITS help desk. If you've worked for CDU before you know it's not called that.
5:52 Now let's look at some phishing websites.

5:56 Legitimate websites are easy to copy, that means it's easy to create a phishing website.

6:04 Generally, the only clue is the web address. So let's have a look at the web address of these two websites.

6:11 The one on the left has cdu-mailcdueduau.webs.com and the one on the right has cdu-mail.cdu.edu.au.

6:23 So the one on the right has a legitimate ending and the one the left doesn't. So that makes it the fake and the one on the right the genuine one.

6:33 What can I do to help?

6:35 Look closely at all emails you receive.

6:39 Mistrust all emails that request your details.

6:44 Look closely at any links on an email and where it is taking you.

6:48 Not only the visible address but the underlying address as well, remember hover your mouse over the link and it will show the real address it going to take you to.

6:58 Legitimate CDU emails should have cdu.edu.au in the address at the end.

7:05 If you come across any suspicious emails forward them to spam-report@cdu.edu.au and our Systems Team will have a look at those and check them out.

7:18 Thank you.

7:20 Hopefully with the information contained in this short video you will be better equipped and have a fuller appreciation of the problem of spam and phishing emails.

7:27 This is a battle that ITMS cannot fight alone and requires the assistance of all staff at CDU.

7:33 Together we can play a part in reducing the amount of spam and phishing emails the world faces.

7:40 So if you want to contact us, you can call the ITMS Service Desk on 89466600. You can log a job with logit and put in logit.cdu.edu.au into your web browser or you can forward any suspicious emails to spam-report@cdu.edu.au .

8:05 Now remember, ITMS will not ask for your username and password via an email.

8:12 This was produced by the Office of Information Technology and Support at Charles Darwin University. Spoken by Andrew King.

8:19 end