

# Scam Detection And Prevention

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

# Disclaimer

This is *not* a “how-to” lesson in scamming

This is a “know your enemy” knowledge transfer workshop

So, what is  
scamming?

# Overview

Scamming is the process by which an attacker manipulates the victim into giving or performing some good or service under bad influence

*Psychological attacks*

With increasing ways to contact people, scamming has adopted more varied attack vectors

*Phishing Emails*

*Scam Telephone Calls*

# Process

Approach: how the scammer falsely prevents themselves to gain trust of the victim

Communication: how the attacker communicates their legitimacy to the victim

Payment: the reward the attacker is looking to get from scamming the victim

# Phishing

*Phishing* is the process by which a scammer will try to coerce you into clicking on a link or downloading a file to capture login information, spread viruses, or implant malware

Attack vector is usually through email, but could also be SMS message, social media post, or advertisement/popup

Payment is whatever you give them!

# Phishing Email Indicators

## Your account has a debt and is past due

☆ Letitia Madden To: jriley ✓

📎 12/16/15, 12:49 PM

Dear Customer,

Our records show that your account has a debt of \$436.{rand(10,99)}}. Previous attempts of collecting this sum have failed.

Down below you can find an attached file with the information on your case.



SCAN\_INVOICE\_33566292.zip



## Your account has a debt and is past due

☆ Letitia Madden

12/16/15, 12:49 PM

Dear Customer,



Sites will usually use your real name.  
Rarely will it just be "Customer".

Our records show that your account has a debt of \$436.{rand(10,99)} Previous attempts of collecting this sum have failed.

Down below you can find an attached file with the information on your case.



Attacker has left in some code.  
Choosing random digit from 10-99.



Beware of ZIP attachments.  
Invoices would usually be PDF.



SCAN\_INVOICE\_33566292.zip



Not to scale. 🐟

**From:** "Cameron Smith via DocuSign" <[dse@docusgn.com](mailto:dse@docusgn.com)>  
**Subject:** Completed: [pagerduty.com](https://pagerduty.com) - Wire Transfer Instructions for  
**Date:** May 9, 2017 at 7:35:49 AM PDT  
**To:** <[@pagerduty.com](mailto:@pagerduty.com)>  
**Reply-To:** "Cameron Smith via DocuSign" <[dse@docusgn.com](mailto:dse@docusgn.com)>

**Document Ready for Signature**



Your document has been completed

**REVIEW DOCUMENT**



From: "Cameron Smith via DocuSign" <dse@docusgn.com>  
Subject: Completed: [pagerduty.com](http://pagerduty.com) - Wire Transfer Instructions for  
Date: May 9, 2017 at 7:35:49 AM PDT  
To: <[smc@pagerduty.com](mailto:smc@pagerduty.com)>  
Reply: "Cameron Smith via DocuSign" <dse@docusgn.com>

Document Ready for Signature



Not the real docusign.com domain!



Hover over and see link goes to  
<http://.../file.php?email=...>



REVIEW DOCUMENT



## We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply [restart your membership](#) to enjoy all the best TV shows & movies without interruption.

**RESTART MEMBERSHIP**

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

—Your friends at Netflix

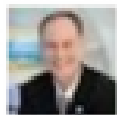
Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

## Urgent Request



Inbox x



Mr. Spenceman <[redacted]>

7:50 AM (1 hour ago) ☆



to me ▾

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.



# Phone

Phone scamming is the process by which a scammer will impersonate an authority figure or trusted source to have the victim divulge personal information, financial data, or to coerce the victim into transferring the attacker money

These scams can potentially go over a longer period of time, payment is usually your information or money

# Phone Scam Roleplay

# Prevention: SIGINT

You can use an app on your phone to alert you when a call seems suspicious or comes from a number reported to be suspect

→ Call Control

You can use a service to monitor incoming email for signs of scamming and filter it out of your inbox

→ Spamfence



# Prevention: HUMINT

Don't engage with unsolicited offers, calls, emails, or other propositions

→ Think before you click or answer

Do be wary of pressured propositions or seemingly innocent requests

→ Verify authority through a different channel

Don't panic!

→ Scammers prey on irrationality

# Conclusion

Scamming works if people aren't vigilant

If something seems too good to be true, it is. If it seems too harsh to be legit, it's not

Don't assume good things, trust but verify

# References

Australian Competition  
and Consumer  
Commission

PagerDuty Security  
Training

EDTS Consulting LLC

Thank You!