



**TF-CSIRT**  
**TRANSITS**

## **TRANSITS Group Exercise**

Based on ENISA Exercise 11 “Incident Handling in Live Role Playing”

Place  
Date

# Roleplay Rules



**TF-CSIRT**  
TRANSITS

1

In this game, you and your table will play as one character.

2

Read your character card and ask your tutor any questions you may have.

3

Alice will start by making a phone call to one of the other characters in the room.

4

After each call the receiver must decide on an action in the form of a communication to another player (call, email, meeting).

5

You cannot use any information that you did not receive from another player.

6

We will keep going until the incident is resolved or the tutors decide to end.

7

When we are finished, you will be asked for feedback on how the incident was managed.

## The Rulers of Time *(and supporting actors)* for this exercise:

the Tutors



They **know** all, **see** all and can pause / fast forward / reverse **time**.





- A talented young (and underpaid) designer.
- Not very happy at Ads-R-Us, and she has been looking for work for a while.

Today, Saturday morning, she received an email from a potential employer, with a PDF attachment describing the position, but when she opened it, it appeared to be empty.



ADS  
RUS



- Network engineer
- Set-up VPN to allow secure remote working
- Is on duty today to provide general support

He is responsible for the company network.  
He doesn't really understand why Ads-R-Us  
needs a CSIRT function, but thinks that  
ERNEST is a pretty good guy all the same.



ADS  
RUS

- Network administrator and IT Support
- Part-time CSIRT Officer

He is responsible for the company network and software, including the security stuff and he has regular contact with Big-ISP and the software vendors who provide services to Ads-R-Us.

ADS  
RUS





- CEO of Ads-R-Us
- A little stressed about the company finances
- Delegation is his key management skill

He is looking forward to a meeting with a big client on Monday for a new campaign, which he has been told will be ready in time.

Right now he is relaxing at home, as its his daughter's birthday.



ADS  
RUS



- Keen IT student
- Loves tinkering with computers
- Into computer security



He believes in ethical hacking, and often finds security flaws in software. He also believes strongly that commercial companies should be generous to helpful testers like him.





- Head developer at MUNIX
- Ads-R-Us uses MUNIX as their group working tool
- Is aware of some bugs, and is working to fix them



He recently took a phone call from some guy asking for a lot of money to tell him about a bug he'd found. He offered the guy credit in the security advisory, but the guy just laughed and hung up. He looked into it and found the bug, but decided to keep it quiet until he had written a patch.





- CSIRT Officer in the biggest ISP in the country
- On duty today
- BIG-ISP supplies the internet connection to Ads-R-U and the majority of users in the country.

He met ERNEST once at a TF-CSIRT meeting, exchanged PGP keys, and has regular contact with him professionally.





It is Saturday morning, and Alice is working remotely on an important project which is due on Monday. She is trying to access some files on the company server over VPN. She can access the server alright, but the files she left there on Friday evening are missing. So she calls the company helpline.

The administrator on duty (Charlie) will discover that somebody had accessed the server from Alice's account last night and apparently erased the project files of all the users from the file server.



Since Alice's account is a regular user account without sufficient privileges to access or modify another user's data, there seems to be something seriously wrong...

# The Players



WINSTON

CEO



CHARLIE

Network Engineer



ERNEST

Sys. Admin  
CSIRT



ALICE

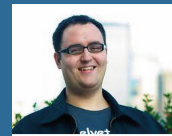
Junior  
Designer



PATRICK

CSIRT  
Officer

MUNIX



STEVE

Software  
developer



KEVIN

Student



**TF-CSIRT**  
TRANSITS

**Thank you**  
**Any Questions?**

3, 2, 1 - Let the exercise begin ...

