# Phishing and Ransomware Attacks in DERs

Matthew De La Rosa, Islam Obaidat, Cori Faklaris, Meera Sridhar

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

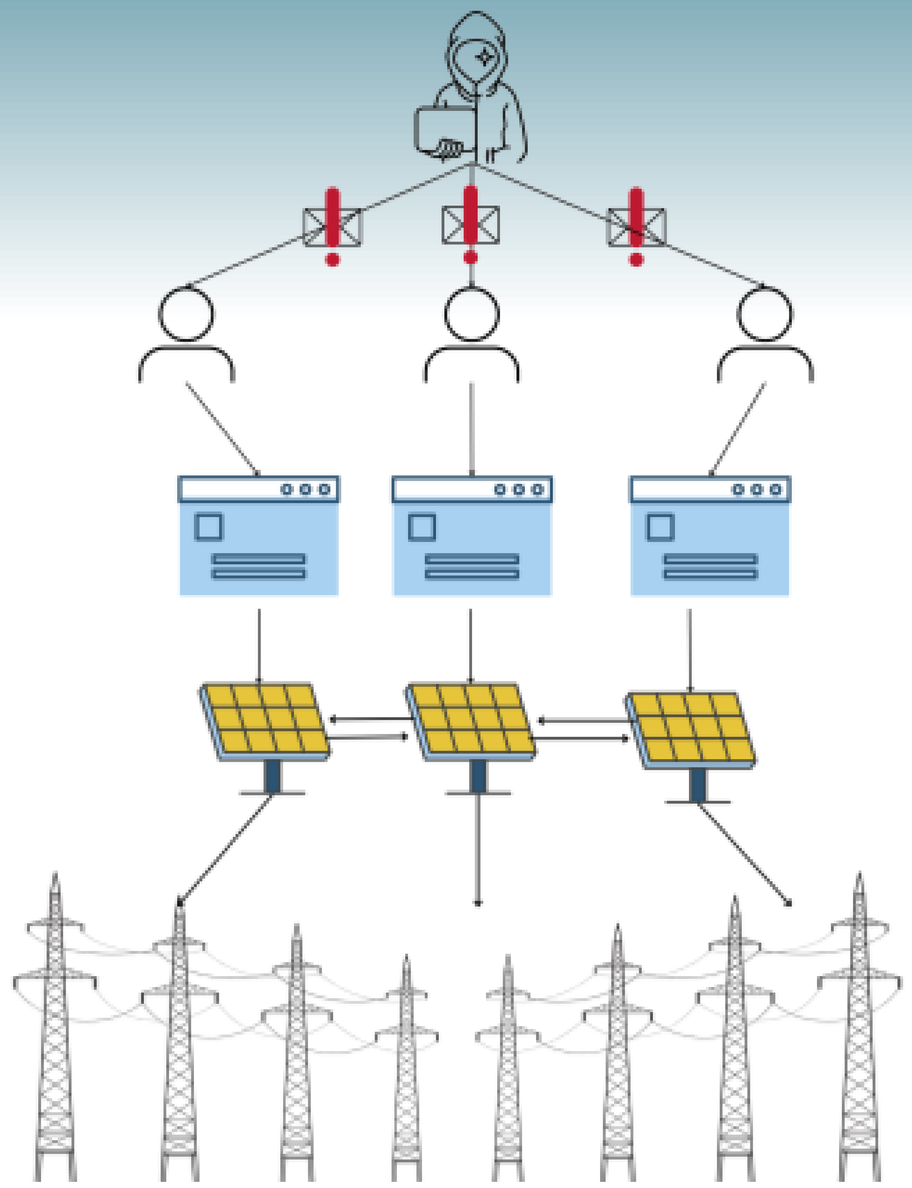
SECURITY + PRIVACY EXPERIENCES GROUP

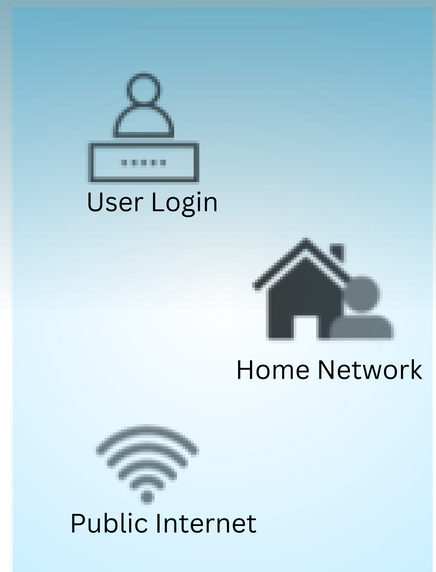
## Abstract

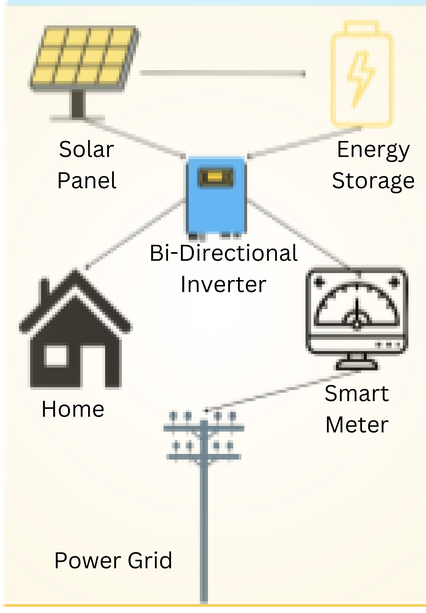
This poster explores the potential security vulnerabilities in Distributed Energy Resources (DER), specifically looking at the Operational and Information Technology components that makeup a DER and what kind of cyber attacks are the most concerning for DER systems.

## What Is a DER

A Distributed Energy Resource (DER) is a decentralized energy source, like solar panels and wind turbines that utilize both Opertional Technologies and Information Technologies to function. DERs improve energy efficiency, reduce transmission losses, and support renewable energy integration, enhancing grid resiliency and sustainability.






## Information Technology (IT)

With DERs being in the hands of the end user, their connection to a local network, and their connection to the open internet there are a lot of potential security flaws that come from the IT components in a DER. The most notable of these are the following.

- The user's login page and credentials.
- The security of the network that the DER is attached to.
- The connection of the DER to the open internet.

## Operational Technology (OT)

Operational Technologies in a DER connect and control the physical power flow within the system. Since they interface with IT components, they are susceptible to IT security threats. An attack on these components could severely impact the DER system as a whole. OT components can be Energy storage devices, Smart meters, Bi-Directional Inverters, and Energy generators.

## Phishing

Phishing attacks could have a huge impact on DERs According to Verizon 2023 DBIR* Phishing attacks and related attacks are involved in nearly **75%** of cyber security incidents in energy infrastructure.

## Ransomware

Depending on the scale, Ransomware attacks could impact entire regions due to DERs. According to Verizon 2023 DBIR* nearly **25%** of cyber incidents on energy infrastructure result in ransomware infected machines.

## Further Research

Due to the novelty of this technology and its potential impact on critical infrastructure, further research is necessary to ensure its security. In this context, researchers should pay specific attention to the following topics.

- To what extent Ransomware impact DERs and the energy grid as a whole
- How DER users can protect themselves against phishing attacks and what malicious actors could achieve with a successful phishing attack
- How can both Operational and Information Technology be designed in a secure manner as well as be maintained and operated in a secure manner