Volume I Issue 11

Date : 16-02-2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Doxing—The Weaponisation of Personal Data

Online Doxxing

The word “doxing” (also spelled "doxxing") is derived from the term “dropping dox,” or “documents.” Doxing is a form of cyberbullying that uses sensitive or secret information, statements, or records for the harassment, exposure, financial harm, or other exploitation of targeted individuals.

This doxing meaning involves taking specific information about someone and then spreading it around the internet or via some other means of getting it out to the public. This practice has been fervent for many years, simply because documents contain permanent records of facts about people and things they have done and said, which can be powerful weapons against them. However, the term “doxing” first gained popularity in the 1990s when hackers began dropping docs on people who had been hiding behind fake names. In this way, hackers could expose other attackers with whom they had been in competition. Removing their anonymity left them exposed to authorities and others trying to track them down.

Doxing has taken a prominent role in modern culture wars, which involve people targeting those who support a cause or hold a belief that is in opposition to one they are trying to push forward

> Doxers can extract personal data from seemingly harmless social media posts
>
> : **Cybersecurity experts**

How does Doxing work?

Doxing is based on the fact that nearly everyone has data about them floating around on the internet, protected by varying levels of security—and in some cases, barely any at all. Once this data has been found, it is weaponized and used against the target.

People often use the same or similar usernames on different accounts for a variety of websites and web applications. It is relatively easy therefore for cyber criminals, activists, or others to use the usernames you have to pinpoint accounts that belong to you. Data from each of these accounts can be taken to compile a more thorough portfolio of documents that reveal information about you

What information are Doxers looking for?

1. **Phone numbers**: These can be used to contact the victim directly while pretending to be someone else and then asking questions to get more information. They can also be used to gain access to secure user accounts.
2. **Social security numbers**: A social security number is required to validate the identity of a person on a variety of websites and with a wide array of companies that hold private data.
3. **Home address**: Not only can a home address be used to verify someone's identity while trying to gain access to a private account, but it can also be used by an attacker to apply for new accounts while pretending to be the victim.
4. **Credit card details**: Credit card information can be weaponized for profit or to harm a victim's credit rating, as well as gain access to other sensitive information.
5. **Bank account details**: Because bank account details are typically only available after someone has satisfied security measures, they can be used to "verify" your identity for someone pretending to be you. They can also be levied to transfer money from your account to someone else's or published in a doxing attack to make the target more vulnerable.

How to protect against Doxing?

Secure Password Protection

Strong passwords are critical for protecting against doxing attacks. For optimal security, passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols with at least 8 characters in length. Using distinct passwords for each account is vital to ensure that if one password is exposed, other accounts remain secure.

Check out our blog post for password best practices.

Multifactor Authentication

Two-factor authentication (2FA) and multifactor authentication (MFA) add extra layers of security by requiring users to provide a username/password combination and another form of verification, such as a code sent via text message or email, before they can access their account. This makes it much more difficult for attackers to gain unauthorized access, even if they manage to get hold of someone's credentials through doxing or other means.

Limit Information Shared Online

Another way to protect yourself from doxers is by limiting the personal information you share online, particularly on public forums, social media sites, or discussion boards where people may search for targets using keywords related to location, job title, or interests. Be mindful when posting photos, too – avoid including details that could identify where you live or work unless absolutely necessary.

Not only is it essential to safeguard your information but also that of those around you. Friends and family members who might not understand how easy it can be for malicious actors to find their personal details should also be educated about good digital hygiene practices.

Doxing is scary because it involves exposure of potentially sensitive information to the public in a way that could damage the victim's reputation or expose them to theft or identity fraud. A doxing attack can also be used to blackmail the target or to embarrass someone's family or friends. Further, doxing can be a weapon for getting someone fired from a job due to things they have done that their employer disagrees with.