Cyberattacks: A growing threat to the US

Recent data reveals **cyberattacks as the most widespread means of stealing personal information** nationally.

Across the U.S., publicly reported **cyberattack-linked data breaches have increased by 27% since 2020**, with **phishing and ransomware breaches emerging as the primary methods**, according to data compiled from the Identity Theft Resource Center.

The number of **phishing and ransomware incidents reached 215 this year**. The rise of cyberattacks juxtaposes a stark decline in physical attacks, especially document theft.

**Document theft has declined by nearly 75% since 2020** with **only six reported instances.**

Despite this, citizens across the U.S. still see information theft as physical – focusing efforts on document disposal. Last November, a D.C.-based community group announced, via its online newsletter, that it would host another document shredding event and mentioned including electronic disposal in future events.

However, data suggest that including electronic disposal would not mitigate residents’ risks of identity theft.

This year alone, **physical attacks made up less than 3%** of reported breaches, compared to the **87% cyberattacks accounted for**.

To combat growing cybersecurity challenges, Identity Theft Resource Center President Eva Velasquez said in a press release, “Everyone needs to continue to practice good cyber-hygiene to protect themselves and their loved ones as these crimes continue to increase.”

Ready.gov’s page on cybersecurity expands on Velasquez sentiment. It describes online practices citizens can take to protect themselves. This includes crafting longer passwords with specialized characters and not clicking on links sent from unfamiliar email addresses.

Ultimately, cyberattacks aren’t just a threat to private citizens. Last November, the surge in cyberattacks prompted a congressional hearing on importance of bolstering U.S. cybersecurity.

Rep. Bennie Thompson, D- Miss said that the government was made aware late last year that the Russian government gained access to government and private networks, and Microsoft later reported the Chinese government had gained and maintained access to Microsoft Exchange Servers.

Jen Easterly, director of the Cybersecurity and Infrastructure Agency, said that 85% of critical cyber infrastructure is in “private hands.

A new body, the Joint Cyber Defense Collaborative, will gather organizations across the government and private sector to coordinate U.S. cyber-defense plans.

<https://docs.google.com/spreadsheets/d/1680gQqxz_gdZPbOAe5eMaRCLomk45GIlZEbdg6Y3jyM/edit?usp=sharing>