19th December, 2024.

Paper Presented by Inemesit Dike at the Nigerian Bar Association Women Forum. (Abuja Chapter)

Topic: Enhancing Female Lawyers' Digital Literacy Against Gender-Based Violence

INTRODUCTION

Legal professionals are increasingly relying on digital tools to conduct work. Whether it's communicating with clients, managing case files, or researching legal precedents. However, with this growing dependence on technology comes the rising threat of cyber risks, which can have serious implications for both lawyers and their clients.

For female lawyers, particularly those handling sensitive cases such as gender-based violence (GBV), these digital threats are even more pronounced. The very nature of these cases often puts lawyers at the forefront of targeted attacks aimed at intimidating or silencing them. Cyber threats, such as data breaches, surveillance, and harassment, not only jeopardize the personal safety of lawyers but also compromise the confidentiality of vulnerable clients.

Protecting your personal and professional data is not just a matter of security. It is essential for upholding the trust and safety of the individuals we represent. By understanding and addressing these risks, we can create a safer, more secure environment for both ourselves and our clients.

Privacy is everyone's responsibility but legal practitioners have a higher responsibility to maintain client confidentiality. The excuse of lack of technological skills or even a breach does not alleviate one's responsibilities.

For female lawyers, digital safety is a critical aspect of professional and personal well-being. Protecting sensitive client data, preserving the integrity of legal work, and ensuring personal safety in the face of digital threats are not optional—they are essential. As the legal landscape continues to evolve in the digital age, female lawyers must be proactive in securing their digital environments to navigate this ever-changing and often perilous terrain.

Digital Threats Lawyers Face

Lawyers face several digital threats in today's technology-driven world. These risks are increasing as more legal work moves online and as cybercriminals target high-value industries like law firms.
Some key digital threats that lawyers face;

● **Phishing Attacks**: lawyers are often targeted by phishing campaigns where attackers pose as trusted sources (e.g., clients, colleagues, or vendors) to trick them into revealing sensitive information, such as login credentials or financial details. Phishing can lead to compromised accounts and financial losses.

● **Surveillance**: This threat is particularly serious for lawyers due to the nature of their work, which often involves privileged and confidential client information. Unauthorized surveillance can take many forms, and it can occur both through direct interception of digital communications or through the use of physical surveillance methods. Regardless of the approach, the impact on the lawyer, the law firm, and their clients can be severe.

● **Data Breaches**: Data breaches are one of the most significant and concerning digital threats faced by lawyers and law firms today. These breaches often involve the unauthorized access, theft, or exposure of confidential client data. Law firms are particularly attractive targets for cybercriminals because they handle highly sensitive and valuable information, such as personal, financial, medical, and business-related data.

● **Online Harassment**: Online harassment is a serious digital threat to lawyers, particularly those handling high-profile, controversial, or sensitive cases. It involves a range of harmful behaviors, including threats, trolling, doxxing, and cyberstalking, all designed to intimidate, discredit, or silence lawyers. It comprises of Threats of Violence or Harm, Trolling and Disinformation Campaigns, Doxxing: Exposure of Personal Information etc.

● **Spyware**: This is malicious software used to steal or monitor data. Spyware is a significant and growing threat to lawyers due to the sensitive and confidential nature of the information they handle. In the legal profession, where confidentiality, integrity, and security are paramount, spyware poses severe risks to client privacy, case integrity, and even the safety of lawyers. Spyware can take several forms, from simple keyloggers that track keystrokes to sophisticated remote access tools that allow cybercriminals to monitor every aspect of a lawyer's digital activity.

Best Practices for Digital Safety

The currency of trade in our profession is Trust and GBV clients are one of the most vulnerable in society.
One must pay attention to the fact that GBV situations are multi-rooted and multi-faceted in the effects.

Be aware of your environment: Don't use Clone buddies that look like USB chargers, use
VPN, Data blockers, etc if unsure, don't charge your devices in public outlets, don't log on to public WiFi with your official devices, be alert against keyloggers and Network sniffers, separate official devices from personal devices, maintain privacy even on one's personal

social life and social media, get anti-virus software for official websites.

Be NDPR and GDPR compliant.

Practical Tools and Techniques for Online Security

1. **Device Protection**:
 • VPNs (e.g., NordVPN, ExpressVPN): Encrypt internet traffic and protect online activity.
 • Antivirus Software (e.g., Bitdefender, Norton): Safeguard against malware and spyware.
 • Two-Factor Authentication (2FA): Add an extra layer of security to online accounts.

2. **Securing Client Information**:
 • Document Encryption (e.g., VeraCrypt): Encrypt files before sharing them.
 • Secure File Sharing (e.g., Signal, ProtonDrive): Use platforms that prioritize privacy.
 • Cloud Storage (e.g., Google Drive with 2FA, Tresorit): Opt for services with strong security features.

3. **Online Safety Tools**:
 • Secure Messaging Apps (e.g., Signal, WhatsApp with encryption): Protect sensitive communications.
 • Password Managers (e.g., LastPass, Dashlane): Create and manage strong passwords securely.
 • Social Media Privacy Settings: Regularly review and adjust settings to limit exposure.

Staying Safe Online - The Call to Action

Taking the Next Steps in Digital Security

1. Prioritize Digital Safety:
 • Assess current security practices and identify areas for improvement.
 • Commit to implementing best practices for digital safety immediately.
2. Next Steps:
 • Sign up for digital safety training programs.
• Start using recommended security tools such as VPNs, encrypted apps, and password managers.
 • Share knowledge and tools with peers to foster a secure professional community.
3. Resources and Support:
 • Reach out to The Legal Concierge for guidance or workshops.

Presented by
Inemesit Dike,
CEO, The Legal Concierge Limited.

THE LEGAL CONCIERGE
Office: 1st Floor, Mina Morrison Centre,
86 Olu-Obasanjo Road, Port Harcourt,
Rivers State.
Email: info@thelegalconcierge.org
www.thelegalconcierge.com
Tel: +2348033010052