Legal Computer Consultants

CYBER SECURITY POLICY

KEEPING CONFIDENTIAL AND CLIENT-PRIVILEGED DATA SECURE

Our law firm is implementing cyber-security policies and best practices to improve network security and protect confidential work-product. Please review, print and sign this policy statement, and return to the office manager immediately.

Password policy:

Do not use the same password for different sites.
Passwords must be strong.
Strong passwords should:
• Contain at least 8+ characters,
• Include upper and lower-case letters, numbers and special characters,
• Not be reused on multiple account logins,
• Changed every 60 to 90 days,
• Never shared with anyone else,
• Do not write passwords on paper. Save in an encrypted application. like: https://start.1password.com
• **USE MULTI-FACTOR AUTHENTICATION (MFA)** on all email accounts and any accounts that store financial information, including credit card information.

Be Careful when you click: prevent RansomWare, Viruses and Key Logging:

Do not click on any link or scan any QR-Code unless you know you can trust the source.
If you are unsure about a link, delete the email and go directly to the website, or call the sender prior to clicking on suspicious links.

Do not share confidential information or credentials:

Social engineering or "phishing" is a non-technical approach hackers use to get sensitive information. Social engineering techniques include spoofing email addresses, fake phone calls, and physical impersonation.

- Setup multi-factor authentication with financial institutions and email hosts to prevent unauthorized wire transfers and unauthorized password resets.
- Setup bank/credit card alerts to notify about transactions. Require verbal approval to emailed instructions to wire money.
- Never click on links asking you to update your credentials for any web site. Instead, even if you think the email may be legitimate, go directly to the website to check and update credentials.
- Never provide security or personal information over the phone or by email to anyone.
- Passwords should never be shared.
- Legal Computer Consultants will never call you to ask for your password over the phone. If you do need to provide confidential credentials, hang up and initiate the call back to LCC. Assume anyone requesting confidential information is an imposter.

Secure your PC

Always lock your computer before leaving your desk: Press the [Windows Key]+[L] to quickly lock your screen.
Do not use USB memory devices on office PCs to save or open files.
Keep devices updated with the latest security updates.

Be careful on WiFi and using other computers:

- If you must login from a strange computer, open the web browser in 'safe mode' or 'private browser'. This prevents your credentials from being saved. Make sure you do not opt to save passwords in the browser. Follow the prompts to fully log out (versus just closing the browser).
- Logging in to strange Wifi is risky: Use a personal hotspot from your cellphone for WiFi if logging in or viewing confidential work product.

Appropriate Use:

- Report any suspicious activity or security concerns immediately.
- PCs and the computer network are the property of the employer and should only be used for business purposes. Do not install software (like streaming music) or use personal email.
- Do not use the computer (including browsing the Internet) for personal use.
- Misuse of PCs may incur disciplinary measures including the potential termination of employment.

Agreement to follow cyber-security policy

I understand and agree to abide by these cyber-security policies.

_____ _____

Signed Dated

Legal Computer Consultants

Clues that may indicate you have been hacked

Device Behavior

1. **Unusually Slow Performance**: Your device suddenly becomes sluggish, freezes, or crashes often.
2. **Unexpected Pop-Ups**: Intrusive ads or alerts appear frequently, even when not browsing.
3. **Programs Opening on Their Own**: Applications launch without your input.
4. **New Toolbars or Apps**: Unrecognized software, browser toolbars, or extensions appear.

Account Activity

5. **Unusual Login Alerts**: Notifications about logins from unfamiliar devices or locations.
6. **Changed Passwords**: Account credentials no longer work, indicating someone changed them.
7. **Emails Sent Without Your Knowledge**: Friends report receiving strange messages or spam from you.
8. **Unauthorized Transactions**: Suspicious charges on financial accounts or unexplained withdrawals.

Security Warnings

9. **Antivirus or Security Alerts**: Warnings about malware or unauthorized access.
10. **Browser Redirection**: Your searches redirect to unfamiliar or malicious websites.

Network & Connectivity Issues

11. **High Data Usage**: Unexpected spikes in your data usage could indicate a hidden process.
12. **Unknown Devices on Your Network**: Unfamiliar devices are connected to your Wi-Fi.

Personal Files & Settings

13. **Missing or Corrupted Files**: Files disappear, are renamed, or become inaccessible.
14. **Unrecognized Changes**: New settings or configurations appear on your device or accounts.

Other Warning Signs

15. **Disabled Security Features**: Your antivirus, firewall, or other protections are turned off without your input.
16. **Fake Antivirus Warnings**: Alerts urging you to download software that you didn't initiate.
17. **Locked Out**: Ransomware messages demanding payment to unlock files or devices.

1. Shut down computers that are not being used.
2. Change work and personal passwords:
    a. Computer and office network passwords
    b. Email passwords, for example;
        i. Office 365
        ii. Gmail
    c. Financial websites, for example;
        i. Banks
        ii. Credit Cards
        iii. Brokerage accounts
        iv. Accountant/Payroll Service portal
        v. Venmo / Paypal / Zelle
    d. Line of business websites and software applications, for example;
        i. Accounting/QuickBooks
        ii. Case Management
        iii. Document
            1. Dropbox/GoogleDocs
            2. ShareFile / DocuShare
        iv. Time and Billing / practice specific
        v. Website Hosting
    e. Commercial websites with your credit card information, for example;
        i. Amazon
        ii. E-Bay
    f. Social Media, for example;
        i. Facebook
        ii. YouTube
        iii. Instagram
3. Reboot the computer you are working on and report if you see any applications stating that you do not recognize.
4. Schedule a scan for viruses and malware.
5. Check email accounts online and Outlook for any rules to forward emails.
6. Review and monitor recent online purchases and financial transactions.

If you suspect your computer or office network has been hacked:

1. Shutdown suspected hardware
2. Disconnect the network from the Internet
3. Schedule a virus and malware scan

Train staff to adhere to cyber-security policies.

LCC will continue to monitor your situation.