CAMPUSGUARD®

Protecting Your Data Privacy

For Consumers

With the recent upsurge of data breaches, consumers are tasked with ensuring their own data privacy now more than ever. Knowing how your data is being used and actively engaging in the following steps will help protect your data privacy.

1 Use Strong Passwords

Create unique, complex passwords for each account. Change passwords every 90 days.

2 Enable 2-Factor Authentication

Use multi-factor authentication whenever possible to add a layer of protection that verifies you as the user instead of an unauthorized user.

3 Utilize the Latest Anti-Virus Software

Set up automatic updates, so anti-virus software checks for updates and scan your devices automatically.

4 Only Use Secure Connections

Do not connect to public, unsecured Wi-FI networks. Only connect to trusted, private networks, or VPN.

5 Restrict Your Personal Info on Social Media

Keep your personal information private. Become familiar with privacy settings and make your account as secure as possible.

6 Limit the Personal Data You Share

From surveys to forms, be mindful of the personal data you are sharing. Is the organization you are giving your data to trusted? Is the information they are asking for necessary? Read their privacy policy to see how your information is stored and shared.

7 Engage with Email Carefully

Phishing emails are a common way for cybercriminals to steal your personal data. Here are tips to avoid becoming a victim of a phishing email:

- Do not open emails from unknown senders.
- Do not click on or open emails with suspicious attachments or links.
- Do not send sensitive information or payment details via unencrypted emails.
- Be wary of emails that urgently ask you to take immediate action.
- Hover over a link to see if the URL is suspicious.
- Do not open emails where spelling and grammar mistakes are present.
- Don't engage with emails that ask for login credentials, sensitive data, or payment information.
- Report phishing emails to your organization's IT department and to the FTC.