Cyber Security Checklist

McGriff Insurance Services

Working Together to Prevent Fraud and Protect Your Data

Even with tremendous investments in cyber security, the most prevalent way for hackers and fraudsters to gain access is to exploit human behavior through social engineering or simply uncovering information that hasn't been well protected by a consumer.

We understand it's hard to keep up with all your accounts and your distributed digital footprint, and that's why we have a simple cyber security checklist to help you avoid becoming an easy target for hackers and fraudsters.

1. Use strong passwords and protect them

- Create long passwords that contain symbols, numbers, and uppercase and lowercase letters
- Don't store your passwords anywhere
- Don't reuse or recycle your passwords
- Don't share your passwords with anyone
- Change your passwords using a randomly generated schedule
- Ensure that your passwords bear no resemblance to former passwords

2. Opt in to multifactor authentication when available

Multifactor authentication requires additional verifying information to grant access to an account. This gives your accounts an added layer of security. Multifactor authentication can include:

- SMS or email notifications
- Biometric identification
- Tokens

3. Avoid links from unknown sources in text, email, instant message, social media and websites

- Be suspicious of any message that asks you to provide personal information. McGriff and BB&T never use emails or text messages to solicit your personal information.
- Hover your mouse over hyperlinks to inspect their true destination
- Make sure you're on the right site before entering personal information - such as your name, address, birth date, Social Security number, phone number or credit card number
- Report suspicious email that claims to be from McGriff or BB&T to InternetFraud@BBandT.com
- Learn as much as you can about phishing

4. Limit what you share on social media and who can view your profile

This gives your accounts an added layer of security. Multifactor authentication can include:

- Your birthdate
- Your street address
- Geotagged photos
- The time you’re away on vacation

5. Secure your devices
   - Always keep your device's software updated (use the latest operating system and browser versions available)
   - Install security software and keep it up to date
   - Download apps from trusted app stores
   - Turn off Wi-Fi/file sharing/AirDrop options when not in use
   - Avoid working with personal or sensitive data when you're using unsecured, public Wi-Fi

6. Secure your important documents
   Protect your Social Security cards, passports and birth certificates by storing them in a secure place such as a safe deposit box, and only carry them when you need them for a specific purpose.

   This information can be used by an identity thief to commit fraud like taking over your financial accounts, opening new loans and credit cards, and establishing utility services in your name.

7. Shred Documents containing personal/financial information
   When you're done reviewing your paper documents like your receipts, financial statements, or credit card bills, put them in the shredder instead of the trash.

8. Order your credit report annually from each credit bureau
   Best practice: Order a free copy once a year from AnnualCreditReport.com and from a different bureau (Equifax, Experian, TransUnion) every four months so that you're always covered.

9. Keep your contact information up to date with McGriff
   Update your email, mobile phone and mailing address in your McGriff accounts.

10. Opt in to security alerts, and promptly respond to the notifications you receive
    If you haven't done so already, set up alerts to keep tabs on your account.