EDGE
CAPITAL GROUP

EDGE INSIGHTS & SERVICES

Protect Yourself, Protect Your Data

Cyber Crime is Spreading

Introduction:

With the COVID-19 pandemic impacting the globe, opportunistic cyber criminals are leveraging our fear and need for information to gain access to individuals' computers and personal information through phishing and other spoofing schemes. These major threats require risk mitigation, risk management and/or risk transfer strategies as the crisis unfolds.

Step 1: Be Wary

Email Scams: About 90% of all cybercrime starts with an email. Check the sender's address and be skeptical of anything that doesn't look or feel right. If it doesn't look right, don't open it. "When in doubt, delete it out."

Invoicing Scams: Scammers will monitor personal news (births, deaths, new homes and more), and then send fake invoices for payment. For example, after finding a widow on the Internet, scammers will pretend to be a collection agency calling about the recently deceased's debts.

Charitable Donation Scams: Beware of requests for money immediately after a disaster. Scammers set up fake websites with names similar to real charities, and solicit donations.

Investment Scams: Scammers will set up seminars or websites where they suggest investing in specific funds or in unusual assets which have made them wealthy.

Personal Scams: With so much information now available online – through social media or online dating apps – scammers may be using blackmail or personal scams in addition to just economic scams.

Small Business Scams: About half of all small businesses experience a cyberattack because they generally have a moderate amount of data and often have minimal cybersecurity.

COVID-19 Related Phone Scams and Phishing Attacks: It is being reported that callers claiming to be representatives of the Centers for Disease Control and Prevention (CDC) are beginning to surface. These calls are scams. Be wary of answering phone calls from numbers you do not recognize.
Malicious cyber criminals are also attempting to leverage interest and activity in COVID-19 to launch coronavirus-themed phishing emails. These phishing emails contain links and downloads for malware that can allow them to takeover healthcare IT systems and steal information.

Step 2: Do These Ten Things Now

START by incorporating these behaviors into your digital life:

1. Do not provide personal/financial information in response to online/offline phone solicitations; **never send money without a phone call and verification**.
2. https: websites that begin with https (as opposed to just http) have a layer of encryption called the secure sockets layer, or SSL. **Never enter your credit card information or other sensitive data into a site without the "s."**
3. "Remember password" functions should always be turned off on your computer. **Never auto-save your username and password information.**
4. **Do not access financial or other accounts from mobile devices or through public Wi-Fi.** Financial transactions should only be conducted on a trusted virtual private network, or VPN.
5. **Disable all "smart home" devices with recording capability** when discussing confidential matters, especially voice activated "smart speakers" such as Alexa, Siri, etc.

RAISE YOUR GAME by using these technology solutions:

6. **Keep computer software up to date**, including firmware on routers and modems.
7. **Install antivirus/malware software** like Norton, McAfee or Total AV on all devices (even your Apple computers and mobile devices.)
8. **Ensure home Wi-Fi networks are secure** – use WPA2 or WPA 3 security and a unique password (call your internet provider if you are not sure what you have.)
9. **Enable security features on any devices and/ or websites** – PINS, fingerprint authentication, facial recognition or multi factor authentication.
10. **Use password management systems** such as Last Pass or Keeper to protect your credentials. These secure websites will help you better manage your usernames and passwords. Passwords should be a minimum of 12 characters and contain a mixture of upper- and lower-case letters, numbers, and symbols.

PROTECT YOUR BUSINESS through training and third-party services:

Small businesses should secure their Wi-Fi networks, train employees on cyber security, and consider using third-party security companies to protect their data. Cyber liability insurance can help a small business survive cyber-attacks by paying for customer notification, credit monitoring, legal fees and fines after a data breach.

ABOUT EDGE CAPITAL

Edge Capital is an SEC Registered Investment Advisor whose objective advice helps individuals and institutions realize their investment management goals. The Edge Strategy Team's thoughtful and timely reports are based on extensive independent research and analysis of firms, financial developments, and macroeconomic trends.

For more research and commentary, visit us online at **www.edgecappartners.com**.

CONTACT EDGE

Phone: 404-890-7707
Email: info@edgecappartners.com
1380 West Paces Ferry Road
Suite 1000
Atlanta, GA 30327

This material represents the views of Edge Capital Group, LLC. This information is provided to discuss general market activity, industry or sector trends, or other broad-based economic, market or political conditions. This information should not be construed as research or investment advice, and investors are urged to consult with their financial advisors before buying or selling any securities. This information may not be current and Edge Capital Group, LLC has no obligation to provide any updates or changes to such information. This material contains forward-looking projections and there is no assurance that these projections will prove correct. Past performance is no guarantee of future success and there is the possibility of lower returns or the possibility of loss.