



THE MACKINS AT BLEAKLEY FINANCIAL GROUP

CYBERSECURITY

ACTIONABLE INSIGHTS BY:

CHRISTOPHER MACKIN, PARTNER AND WEALTH ADVISOR AT BLEAKLEY FINANCIAL GROUP
MIKE ZWEIBACK, CO-FOUNDER ZWEIBACK Fiset & COLEMAN

SEPTEMBER 2021

A person in a dark suit and blue tie is shown from the chest up. Their hands are held out, palms up, in front of them. In the center of their hands is a glowing blue padlock icon. The background is dark and out of focus.

EVERY 11 SECONDS

Experts estimate that a ransomware attack will occur every 11 seconds in 2021.*

The Challenges

UNDERSTANDING CYBER THREATS

It is important to have a deep understanding of cyber threats, the ways you can mitigate the risk, the importance of a business and personal incident plan, ransomware and the vulnerabilities that occur when traveling and interacting with family members.

The reality is that ransomware is now the most prominent cybersecurity threat and the costs are steep. In 2018, the average ransom fee request was \$5,000. In 2021, the average fee request has risen to \$200,000.

Even well-funded companies lack the cybersecurity maturity it takes to prevent a hack.

The landscape and hackers change quickly. Individuals who have a lot to lose from a cybersecurity hack should consider hiring a firm to run a holistic cybersecurity assessment every three to six months.

*<https://www.varonis.com/blog/ransomware-statistics-2021/>

BEST PRACTICES FOR BUSINESS OWNERS



Inventory of authorized devices on the network.



Inventory of authorized software.



Practice your incident response plan — tabletop exercises for your managers.



Continuous vulnerability assessments and remediation.



Monitoring and analysis of audit logs.



Data recovery planning.

NUMBER ONE TIP:

Have a well-rehearsed incident plan

The importance of every business having a well-rehearsed incident plan cannot be overstated enough.

There should never be a hesitation as to who should be called first, what steps need to be taken and when.

During a cyber attack, time is of the essence. There have been plenty of cases where an IT director was notified about a ransomware attack and the system was shut down.

The team mistakenly thought this was the worst of it and hours would go by before other professionals were called. In the meantime, hackers were downloading and stealing more data and information.



PLANNING FOR THE WORST RANSOMWARE — TO PAY OR NOT TO PAY?

Hackers use ransomware tactics because they plan on being paid. In an effort to curb attacks, the FBI is currently advising most businesses to not pay the ransom. But, the reality is that upwards of 90% of businesses who pay the ransom will get their data back.

The caveat here is that the FBI is now considering ransom payment a potential crime. Meaning if you pay for the encryption code to your own data, YOU may be the one committing the crime (i.e.; they may believe you are supporting a terrorist group or something similar)

BEST PERSONAL CYBER HYGIENE TACTICS



- ✓ **What devices are you utilizing?** Bring the fewest number of devices while traveling.
- ✓ **No unsecured Internet traffic!** No auto connections while on the road. Bluetooth and WiFi off.
- ✓ **Use Two Factor authentication.** For remote logins you need to enable 2FA.
- ✓ **Pick up the phone.** Verify transactions by speaking to someone on your staff and do not rely on electronic communication.
- ✓ **Train your staff to make smart choices.** Employees are usually more vulnerable when it comes to online activities and knowing what is safe and vice versa.
- ✓ **Don't use business center computers while traveling.** Passwords are all stored on these open devices as well as any transaction.

Planning to work to
ACHIEVE YOUR GOALS

Advisors associated with Bleakley Financial Group, LLC may be either (1) registered representatives with, securities offered through LPL Financial, Member FINRA/SIPC, and investment advisor representatives of Bleakley Financial Group, LLC; or (2) solely investment advisor representatives of Bleakley Financial Group, LLC, and not affiliated with LPL Financial. Investment advice offered through Bleakley Financial Group, LLC, a registered investment adviser and separate entity from LPL Financial.

Christopher Mackin is solely an investment advisor representative of Bleakley Financial Group, LLC and not affiliated with LPL Financial.

LPL Financial and Bleakley Financial Group do not provide tax advice. Please consult your tax professional on your situation.

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual. All performance referenced is historical and is no guarantee of future results. All indices are unmanaged and may not be invested into directly. 36651-1