Lowenstein Sandler

CYBERSECURITY AWARENESS

KEY TAKEAWAYS FOR PERSONAL ONLINE SECURITY

As working remotely becomes more customary, cybercriminals are more frequently targeting people who work from home. We must now be extra-wary of hackers trying to exploit coronavirus fears to steal confidential financial and medical information. For example, the pandemic has led to a sharp increase in everything from fraudulent e-commerce vendors for masks, sanitizers, and test kits to phony investment sites to email scams ("phishing") and phone scams ("vishing"). Here are some extra steps you can take to protect yourself from a personal cybersecurity attack.

> **According to the FTC, credit card fraud was most prevalent in identity theft cases last year.**

IDENTITY THEFT

- If possible, freeze your credit reports and sign up for an identity theft prevention plan.
- Shred sensitive paper documents.
- Only provide your social security number online when absolutely necessary.
- Only share private information using secure messaging apps.
- Use unique passwords and multi-factor authentication for online services. We highly suggest using a password manager to keep track of them.

If something does happen, stay calm and act quickly:

- Call your banks/financial institutions, but don't use the phone numbers provided in suspicious emails or physical mail.
- File a report with identitytheft.gov.
- Contact law enforcement if necessary.

Lowenstein Sandler

HOME AND TRAVEL SECURITY

- Organize, centralize, and back up your data with a cloud service.
- Make sure your home computer operating system is current (no Windows 8, 7, or XP), and turn on automatic security patching.
- Use strong wireless encryption at home (WPA2), and consider adding a robust anti-malware software package.
- Don't do anything with sensitive documents while connected to a public Wi-Fi; use your cellphone's hotspot instead, whenever possible.
- Don't geo-tag social media posts when on vacation or away from home.
- Consider encrypting your laptop and purchasing a privacy screen for business travel.

ONLINE SHOPPING

- Only use credit cards or PayPal for purchases– no debit cards.
- Shop directly from online stores; don't click on social media ads.
- Never give more information than needed (required v. optional form fields).
- Don't save your credit card information with companies that are not name brands.
- Don't use sites that require personal information to access coupons or discount codes.
- Be vigilant about reviewing your credit card statements on a monthly basis.
- Don't pay credit card bills via email links; pay directly on vendors' sites.
- Be skeptical of any unexpected invoices or requests to pay for anything using gift cards.

SOCIAL MEDIA

- Do not overshare!
- Only accept friend requests from people you know, and clean up your friends lists on a semi-regular basis.
- If you receive an email from a friend about their account being deleted, contact them outside of that platform to confirm.
- Make sure your privacy settings are set so your friends lists, photos, and personal information are hidden from the public. (For your birthday, only share the month and day– not the year.)
- Your name, profile picture, and cover photo are public; remember: whatever you post online stays online!

50% of internet users receive at least one phishing email per day. 1 in 25 users clicks on those emails.

Additional Resources

- Freezing Your Credit: consumer.ftc.gov/articles/0497-credit-freeze-faqs
- Antivirus Software Recommendations: consumerreports.org/cro/antivirus-software.htm
- Cybersecurity & Infrastructure Security Agency: us-cert.cisa.gov/ncas/tips/ST04-013
- Free Credit Report: annualcreditreports.com
- Check to See If Your Email Account Was Hacked: haveibeenpwned.com
- Places to Check for Scams: consumer.ftc.gov/features/scam-alerts
- Top Tips for Parents on Cybersecurity: mw.k12.ny.us/wp-content/uploads/2015/05/Safe_Secure_Parents_Top-Tips_acc.pdf