THE NAVIGATOR
COMPASS
NETWORK GROUP

DECEMBER 2015

In this issue...

5 Tips to Keep your Credit Cards Safe this Holiday

Tis the season to shop till you drop… till you get decked trying to fight a mother of four for the very last My Little Pony, till you get trampled by the horde of shoppers behind you, or till you get buried alive in a pile of wrapping paper and scotch tape.

And, tis the season to suffer from credit card fraud, to have your identity stolen, and your bank account hacked. So while you're out and about, spending hundreds, eating too many calories, and thinking about in-laws, do what you can to save your finances from hitting rock bottom. Here are five tips to protect yourself both online and offline this holiday season.

Know what's going on.

Check your account daily. If someone hacks your account and begins to make purchases, the sooner you notice, the better. Sometimes hackers will charge very small items to your account to see if you're paying attention. It could be 59 cents on Monday morning, $1.02 on Thursday afternoon, and $4.99 on Friday night. If you don't notice, the big charge (or charges) aimed to drain your entire account may be a few hours away. If you notice the odd, standalone 52 cents on Monday afternoon and call up your banking institution right away, you'll avoid a great deal of stress and hassle.

Andrey_Kuzmin / Shutterstock.com

Only carry what you need.

Last year, the average credit card owner in America had up to four separate accounts. In theory, you may have a credit card for Target, Walmart, Lowes, and a general purpose one from a company like Chase or Visa. However, the question is, do you have every card on you at all times? If you're going Christmas shopping at Target, do you still have your other three cards in your wallet? And if you do, why? The only thing you're doing is opening yourself up to a potential for greater financial loss; therefore, it's best to leave your other cards at home in a safe place—and not left behind in a shopping cart somewhere.

Online shop at home.

The point of online shopping is to be able to purchase items from the convenience of your home, but this doesn't mean people don't online shop from outside their home. Maybe on Black Friday you were standing in line at Walmart eagerly awaiting mass hysteria, and you passed the time by purchasing other items on your Amazon app. And of course, you connected to Wi-Fi to do this extracurricular shopping, correct? Most likely. However, when it comes to Wi-Fi, it's important to be extremely picky and extra cautious. Hackers can set up illegitimate hotspots that appear to be nothing out of the ordinary, but as soon as you connect, you've given an outside source direct access to your smartphone and everything it contains. If you're going to connect to Wi-Fi, stay away from any online accounts and financial information.

Look for HTTPS.

This tip is very simple. At home or on-the-go, only purchase from websites with 'HTTPS' rather than 'HTTP'. HTTPS means the site is secure, and your data will be encrypted.

Keep everything up-to-date.

All those devices you have floating around—tablet, phone, laptop, PC, other tablet, second phone—they should be updated 24/7. Updates are there for a reason and in many cases, they are developed to patch security flaws and to strengthen your system. If you consistently postpone updates, you will create holes in your devices that hackers and malware can slip right through. Some devices are set up for automatic updates, and some are not. But most updates are very easy to find, and usually all it takes is a trip to your settings tab. Take the trip before it's too late.

© 2015 Compass Network Group. All rights reserved.

stockcreations / Shutterstock.com

Searching for a good gift under $50? We might have the one for you.

Christmas is right around the corner and you know what that means. It's time to spend some money. And thanks to CNET, we have a list of gadgets under $50 that anyone on your list would love to unwrap.

Here are four of our favorites:

Misfit Flash

This inexpensive activity tracker counts calories, measures distance, tracks steps, and monitors sleep patterns. Misfit Flash can be worn around your wrist or easily attached to a shoe, pocket, sleeve, or keychain and can be purchased in a variety of colors. Your activity is transformed into useful information with the assistance of the Misfit App which is compatible with Androids and iPhones. Misfit Flash is available for as little as $20 and for as much as $200.

Sling TV

This one of a kind streamer can connect to basically any cable alternative. From Roku and Amazon Fire to Chromecast and Nexus (which are all under $50 if you purchase through Sling's website), you can stream Sling TV's 'bundles'. The initial package starts at $20 a month and you gain access to a slew of television channels such as ESPN, AMC, Food Network, CNN, Cartoon Network, and TNT. You can opt in for additional packages like Kids, Hollywood, Lifestyle and Sports at $5 a bundle.

Deck by Sol Republic

Deck is a portable speaker that can stand up to the best of them. It is designed for on-the-go listening so it's built to outstand water, sand, and harsh weather. Deck comes in seven different colors, has a battery life of 8 hours, can connect to Wi-Fi from a distance of 60 feet, and can pair with a Bluetooth connection.

Moshi Mythro Headphones

For $30, give the gift of crisp sound by way of Moshi Mythro in-ear headphones. These aesthetically pleasing headphones are coupled with an integrated push button microphone to answer calls on-the-go. Available in six colors, these silicon ear tips provide "rich and vibrant sound without distortion."

Inbox meet Artificial Intelligence.

No longer do we consider automatic archiving the most sophisticated aspect of our emails. Instead, Google has trained its email platform to respond to emails for you.

Smart Reply integrates AI into your inbox with the support of an arsenal filled with 20,000 short phrases. This new extension allows you to respond to emails quickly and cross items off your to-do list with little effort.

When you open an email, Gmail will "read" the content with you and automatically generate responses for you that directly relate to the content. Google employs a "thought vector" to capture the main essence of the email; this means that one key concept--despite its structure—will point to the same set of responses. An example would be, "Can you make the meeting tomorrow?" versus "Does tomorrow work for that meeting?"

Google attempts to offer users multiple ways to answer questions and respond to requests. If your email reads, "Would you like to have Christmas at our house?" Smart Reply could offer up: 'Count us in!', 'We'll be there!', or 'Sorry, we won't be able to make it.'

Coined as two-tap email on the go, Smart Reply only requires two taps to send an email. A tap to add the phrase and a tap to send the email. If you need to alter the phrase or add to it, that's not an issue. Tap to add your phrase, edit your content, and send it off.

http://googleresearch.blogspot.com/2015/11/computer-respond-to-this-email.html

http://www.wired.com/2015/11/google-is-using-ai-to-create-automatic-replies-in-gmail/

http://gmailblog.blogspot.com/2015/11/computer-respond-to-this-email.html

http://lifehacker.com/inbox-by-gmail-adds-smart-replies-that-predict-what-you-1740260733

GaudiLab / Shutterstock.com

© 2015 Compass Network Group. All rights reserved.

4 Questions You Can Ask To Avoid a Malicious Email

Malicious online activity threatens your professional and personal life on a daily basis. It doesn't take much for a hacker to crack your password and break into your online account or for a seemingly insignificant virus to slip into your network and corrupt every last bit of your data. And, these days, phishing has become a go-to method for many hackers around the world.

All it takes is for one employee to open up the wrong email. One click or one download later and you'll find yourself in the middle of a full-blown attack, whether you realize it now or six months down the road (research from a few years back asserted that it takes companies an average of 458 days to notice an attack).

23% of all people that receive a malicious email open it. To make matters worse, 11% of these recipients take things a step further and open the attachment or click the link contained in the email. Why is this? Because hackers have changed their tactics.

Targeting specific industries, companies, and job titles, Spear Phishing involves significantly more effort on the hacker's end. They spend a great deal of time researching their targets to make their email appear more legitimate and clickable. Because of this, it's crucial to know how to detect malicious emails before you unknowingly invite someone into your network.

Where did it come from?

Always check the sender before you do anything with an email. Ask yourself a few questions. Do you know this person? Why would this person or company need to send you an email? Are you expecting an email from them? Do you do business with them? Have you ever done business with them? For what reasons would this person or company potentially reach out to you? If you can't answer any of these questions, you may want to avoid the email, or at the very least, not open or click anything inside it.

Is there a workaround?

If you open an email, and you feel a little uneasy about what it wants you to click on or to download, try to find a workaround. Can you get to the proposed link in another method? For instance, if it's an email asking you to verify your banking information, there are a few different options. Manually type in your bank's website and go at it from that direction. Or, you can even call your bank and request confirmation. Just don't use any numbers listed in the email because they could be illegitimate.

How does the email look?

The majority of malicious emails have grammar mistakes. If anything looks even a little off, don't perform any action the email asks of you. Verify the company name, contact information, and body of the email for punctuation, spelling, and capitalizations. Avoid emails that look anything like this, "Please verify your online banking cridentuals." Also, carefully review the links. For example, an email asking you to visit www.Targit.com probably isn't legitimate.

What is the call to action?

Sometimes all it takes is a simple question to catch most malicious emails. Take into account the previous scenario with the online banking credentials. Why would your bank ask you to verify your credentials? Do they give you a reason? If they do give a reason, is it a good one? Have they ever asked you to do this before? Has any bank asked you to do this before? Your answers to these questions should guide you to the appropriate response. And, if you still feel hesitant, give your bank a call.

http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/

http://www.wired.com/2015/04/email-phishing-attacks-take-just-minutes-hook-recipients/

http://krebsonsecurity.com/2012/07/email-based-malware-attacks-july-2012/

Bacho / Shutterstock.com

lchumpitaz / Shutterstock.com

A Simple Encryption Application for your Smartphone

Open Whisper Systems, the software group behind Redphone and TextSecure, has released the Android version of Signal. For the last year, Signal has been available to iPhone users and has been personally endorsed by Edward Snowden, the NSA whistleblower who leaked classified information back in 2013 regarding the unauthorized access of American phone records and data.

Signal is a free downloadable smartphone application that encrypts your data from phone calls and text messages to prevent in-transit interception. Previously, Signal for Android was separated into two apps, Redphone and TextSecure and last year, TextSecure was integrated into Whatsapp, a popular smartphone messaging app.

This strategic partnership between Whatsapp and Open Whisper brought TextSecure to over half a billion devices, causing alarm and distress for many government agencies. The British Prime Minister, David Cameron, and the American FBI Director, James Comey, both openly rejected the integration. Cameron threatened to ban the app from Britain altogether, and Comey cautioned Congress about the implications of widespread consumer encryption.

In a video interview, Snowden, however, took another stance regarding the widespread adoption of applications like TextSecure and Signal. He asserted that everyone should be advocates of their personal privacy, even if you aren't doing anything that needs protection. "Even if you're just calling your grandmother…" With the widespread adoption of these technologies, there should eventually be less stigma that surrounds them. Snowden believes this will help create a herd immunity to fend off government ridicule regarding personal privacy.

Signal is free to download. For iPhone users, you can find the application here and for Android users, you can find it here.

© 2015 Compass Network Group. All rights reserved.