G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

DECEMBER 2022

Highlights

Cyber Safety for the Holidays

G2M's Cybersecurity Predictions for 2023 Wrap-Up

Holiday Season is Prime Time for Hackers and Ransomware Demands

2023 Webinar Schedule

Upcoming Conferences

Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.

January 12, 2022
10:00am

Cyber Safety For the Holidays

Posted by Karen Heumann, December 19, 2022

230M US consumers own smartphones and 100M own tablets. Two thirds of consumers plan to use their cell phone or tablet to shop for the holidays. 79% of smartphone users have made an online purchase using their mobile device in the last six months. Here are some security tips:

Safety Tips While Traveling

- **Use a VPN as a hotspot when you go online.** Avoid free Wi-Fi and the security potential risks.
- **Okay, you decided to use free Wi-Fi anyway? Confirm your network.** If you do connect to public Wi-Fi, confirm the name the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
- **Disable auto-connect on your devices.** Manually connect only when you want to.
- **Secure your devices.** Keep track of your electronics. Don't leave your devices unattended.
- **Don't use shared computers.**
- **Okay, you decided to use the shared computers anyway?** Avoid making purchases or logging into email. You don't know if the systems are up to date with the latest security software.

Safety Tips for Shopping Online

- **Update Software.** Make sure your internet-connected devices – including PCs, smartphones and tablets – are free from malware and infections by running only the most current versions of software, web browsers and other apps.
- **Use secure Wi-Fi.** Don't make purchases while connected to public Wi-Fi; instead use a virtual private network (VPN) or your phone as a hotspot.
- **Lock down your login.** Create long and unique passwords and use multi-factor authentication.
- **Resist the urge.** Buy only from trusted and established online retailers.
- **Avoid phishing.** Don't open emails from unknown senders or click on links in messages.
- **Shop securely.** Not only should you make sure your internet connection is secure. Check to make sure you're shopping on a site that uses SSL protection. The easiest way to tell is to check your browser's address bar. Look for https is the URL. Sites without the s are not safe to submit payment information or other personal details.
- **Smart Pay.** Use a credit card or pre-paid debit card instead of a debit card linked to your bank account. Or, use an established third-party payment service, such as Google Pay or PayPal.
- **Monitor your accounts.** Check your online financial accounts regularly for suspicious spending. Take advantage of text and email alerting services to keep track of financial transactions.

G2M's Cybersecurity Predictions for 2023 Wrap-Up

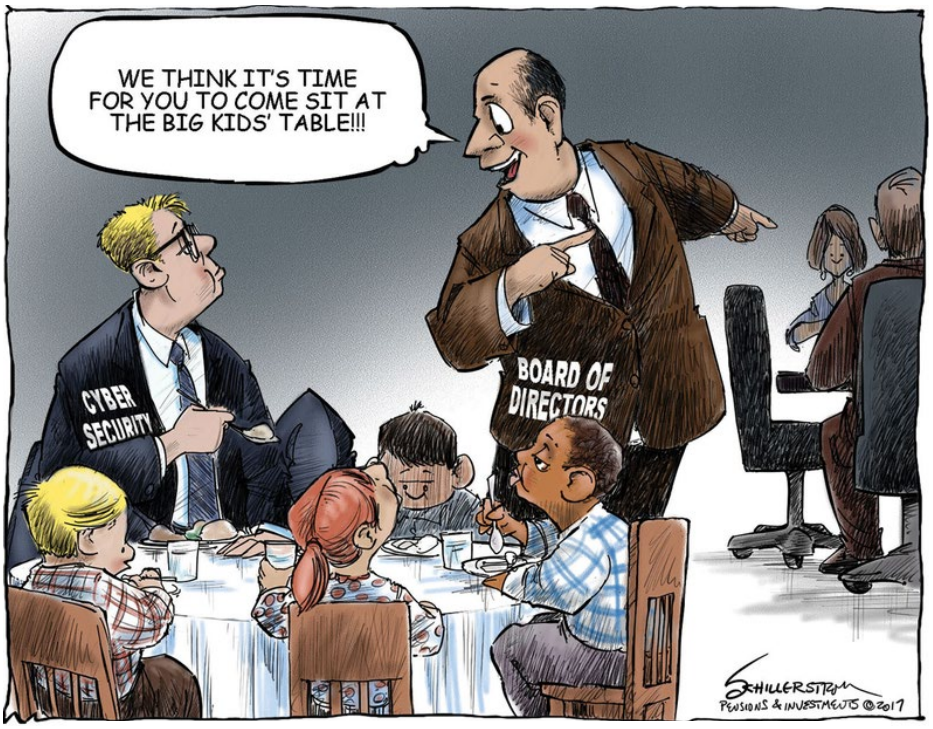
Posted by Mike Heumann, December 19, 2022

Just like any end-of-the-year newsletter, predictions for the following year are not only likely, but expected. In that vein, we thought we would share some predictions from a number of sources on what 2023 might look like for cybersecurity:

- IBM sees prioritized investment in cybersecurity as integral to prevent business disruption and reputational loss from major breaches irrespective of potential economic headwinds.
- Raytheon's Torsten Staab (PhD, Principal Engineering Fellow) predicts that developing and deploying "quantum-resistant" security strategies will become mainstream. While the primary focus will be on asymmetric encryption algorithms such as RSA (which are widely expected to be vulnerable to quantum computers, these algorithms are some of the most widely used today.
- SANS Institute has two predictions regarding cybersecurity workforce trends: i) the skills gap in cybersecurity will continue to grow, and it is an area that most HR departments and professional recruiters are ill-adapted to gauge. The greatest counter to this will be workforce security education, which can significantly increase cybersecurity team effectiveness and retention.
- F5 Labs predicts that "shadow APIs" (either ones that were not meant to be endpoints, or the classical "backdoors") will grow as a risk for large-scale data breaches. This will be magnified by the use of open source software libraries, which are increasingly being targeted as vehicles for malware, or for their vulnerabilities.
- Privacy will become a greater concern in the US according to AT&T as states pass their own consumer data privacy laws. While their primary targets will be businesses exempt from current data privacy acts like HIPAA, PCI DSS, FERPA, and GLBA, expect these frameworks to be comprehensive and with meaningful enforcement mechanisms.
- Forbes predicts that work-from-home cybersecurity will become a (bigger) priority for businesses, especially with the increased use of personal (and often unsecured) devices. Attribution will also become more important as teams increasingly include people that are "strangers", making impersonation attacks more attractive.

- Cyber-Insurance will continue to become more difficult for businesses, according to BeyondTrust. In some cases, it will be because these companies are not cyber-insurable; in others, the increases in cyber-insurance premiums will leave many companies effectively uninsurable for cyber risks.
- One of Venafi's predictions is that Putin's regime will increase its attacks on Western economies as "payback" for Russia's exclusion from the international finance community. This will not only focus on disrupting Western economies, but also generating hard currency from attacks (i.e., ransomware).
- Kevin Lynch of Optiv predicts an increase in the pressure to provide meaningful integration across cybersecurity tools, and that this will become one of the attributes that customers will look at when deciding which tools to keep versus replace.
- HelpNetSecurity believes that the recent Uber data breach criminal convictions will increase the awareness of the liability that CISOs may have under today's regulatory regimes, putting increased pressure on CISOs.
- Collaboration tools such as Slack, Microsoft Teams and OneDrive, and Google Drive will be increasingly targeted according to Check Point Software Technologies, especially as remote work continues to be the norm for most companies.

Beyond this, expect that the impact of "mega-platform" companies such as Palo Alto Networks on the cybersecurity ecosystem will drive more consolidation within the industry and that managed cybersecurity services will continue to eat up market share within the small- and medium-sized business marketspace, especially as a way to get cyber-insurance at something approaching reasonable pricing and coverage.


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS ©2017

Brilliant work by Roger Schillerstrom, Editorial Cartoonist

Holiday Season Is Prime Time for Hackers & Ransomware Demands

Posted by Mike Heumann, December 19, 2022

Businesses are prime targets for cybercriminals during the holiday shopping season. Think about it – most retail companies make the majority of their revenue in November and December (try to find a parking space at the mall during those months!). Hackers know this, and they also know that companies will pay off ransomware attacks during these months for exactly that reason. Historically, attempted ransomware attacks increase by roughly 30% during this time, as reported by Darktrace. If making your year's revenue means keeping (or getting back) the operation of your point of purchase systems (for instance), paying ransomware becomes an easy choice for most businesses.

This problem is also made worse by the fact that most retail-related businesses are exceptionally busy during this period. The Global Risks Report released by the World Economic Forum found that 95% of cybersecurity threats that people have faced have in some way been caused by human error. In addition to staff being exceptionally busy, they are also thinking about the holidays themselves, as well as being generally more tired. Unsolicited emails during the holiday season also increase substantially, giving cybercriminals a greater chance of launching successful phishing attacks. Given that most targets of phishing emails open the emails 70% of the time, the likelihood of a successful attack goes way up during the holiday season. Finally, computer networks tend to be under intense strain due to the increased traffic during the holidays, making the potential for network penetration significantly higher.

In addition to observances for year-end holidays, some organizations elect to shut down for more extended periods of time. For example, nearly half (44%) of U.S. employers responding to Lockton's 2021 HR Trends Survey reported that they closed their doors for Christmas Eve in 2021, and 5% were closed from Christmas through New Year's Day 2022.

Employees scramble during this timeframe – with end of the quarter pressures, end of the year work wrap-up, shopping while shipping windows still meet holiday deadlines, plus colder weather which contributes to the desire to stay under the covers longer each morning (and avoid all of those other pressing stressors.) There is a labor shortage and the people who are present are maxed out. Hackers are aware that there is more valuable data to pounce on during the holidays, so a successful attack would be more rewarding. With increased shopping, retailers have more consumer data. It's no wonder that 24% of attacks target retailers.

Add to this the normal exploits like remote desktop protocols, misconfigured ports, and recent Microsoft Exchange vulnerabilities, and you have a recipe for potential disaster.

ThriveDX explains that an increased risk of cyber attacks during the holidays doesn't mean that your organization should sit back and do nothing and offers the following to protect your business from from cyber threats:

- Training employees to raise awareness about cyber threats to minimize human error
- Identify flaws and vulnerabilities in all your organization's connected devices
- Update all your software
- Add an extra security layer to your enterprise's email accounts
- Make customer service more accessible to address concerns swiftly
- Regularly test your cyber defenses
- Have a robust contingency plan

Stay alert to avoid getting your business hacked, shut down, or otherwise disrupted. And Happy Holidays!

WELL, TIMMY, IF YOU DIDN'T WANT ME TO SEE YOU WHEN YOU'RE SLEEPING, KNOW WHEN YOU'RE AWAKE, KNOW IF YOU'VE BEEN BAD OR GOOD, AND SELL THAT DATA TO THIRD PARTIES, THEN YOU SHOULD HAVE CHECKED YOUR PRIVACY SETTINGS.
TOM FISH BURNE
© marketoonist.com

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. Registration links and more information will be available in our next newsletter, on our website, and you can always contact us directly with questions. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

Interested in Sponsoring a webinar? Contact G2M for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Cybersecurity

Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.	January 12
Cybersecurity for Remote Workers & Mobile Devices	March 23
The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	May 25
xDR- The Promise versus the Reality	August 3
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9

Enterprise Storage & Technology

The Need for Speed: NMVe & Advanced SSDs	February 7
Memory As The New Storage – CXL, Extended Memory, & Persistent Memory. What Does the Future Hold?	March 7
Storage Architectures for Artificial Intelligence & Machine Learning	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27

NVMe & NVMe-oF – Past, Present, & Future	July 11
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Upcoming Conferences

2023

January 5-8	CES, Las Vegas & Virtual
January 18	SNIA Persistent Memory Summit, San Jose, CA
January 30-Feb 1	Cybertech Global TLV, Tel Aviv, Israel
February 6-10	Cisco Live, Amsterdam, Netherlands
February 13-14	Gartner Security & Risk Management, Mumbai, India
February 14-16	ESNA Expo, Long Beach, CA
February 14-17	ITExpo East, Fort Lauderdale, FL
February 27-28	Gartner Security & Risk Management Summit, Dubai
February 27-March 2	Mobile World Congress Barcelona
February 28-March 2	Rice University Energy HPCC Conference, Houston, TX
March 8-9	CloudExpo Europe, London
March 14-16	Gulf Information Security Expo, Dubai, UAE
March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas

April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas
April 17-21	HIMMS Global Health Conference, Chicago, IL
April 19-20	CyberSec Europe, Brussels, Belgium
April 24-27	RSA Conference, San Francisco
May 22-25	Dell World, Las Vegas
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 1-3	Flash Memory Summit, Santa Clara, CA
August 5-10	Black Hat USA, Las Vegas
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results