5 THINGS WE WISH USERS WOULD STOP DOING!

Chelle Clements and Lee Neely
Presented at the SANS Enterprise Defense Summit in Redondo Beach, Ca
WE ARE...

- Chelle Clements - Lawrence Livermore National Laboratory (retired), currently with Online Marketing and Publishing (OMP) developing and maintaining web sites for non-profits
- Lee Neely – Lawrence Livermore National Laboratory, Cyber Security, Senior Cyber Analyst, SANS Analyst and NewsBites editorial board and GIAC advisory board member, Co-host SecurityWeekly podcasts
WHY SHOULD WE ALL BE CONCERNED?

- People make mistakes – poor passwords, web surfing, opening email attachments, etc.
- Information security can’t be guaranteed – the only secure system is turned off, unplugged and in a locked room...maybe...
- Awareness isn’t just a good idea – it’s the law
- Employee churn and learning curves – people come and go, and they need at least annual information security training, if not quarterly
- The threats are always changing – criminals are getting smarter every day

https://www.securedestruction.net/data-security/5-reasons-why-security-training-for-employees-is-essential/
ANOTHER REASON TO BE CONCERNED...

- Phishing dupes a victim into opening an email, instant message or text message (https://www.incapsula.com/web-application-security/phishing-attack-scam.html)

- 30% of phishing emails are opened (Fortinet presentation at 2/27 Boise ISSA meeting)

- 91% of cyberattacks and the resulting data breach begin with a spear phishing email (https://www.csoonline.com/article/3225471/please-dont-send-me-to-cybersecurity-training.html)
OUR CURRENT PERSONAL TOP 5 ISSUES

- Users opening email from parties unknown
- AND then clicking nasty links within the email (phishing!)
- Weak passwords…if the user even uses one
- Users clicking on questionable websites (at home and work)
- Users uploading software that may be contrary to company policy
OH HHHH!
What to do?
SO...THINGS TO THINK ABOUT IN THE WORKSPACE

- Educate your employees
  - Keep cyber security a regular conversation & everyone always needs more training (employee-staff-managers)

- Educate them on what to look for
  - How to watch for fake URL's, be aware of social engineering & securing printer/scanner

- Educate them on using different and smarter passwords
  - Longer is better, do not save them to browsers, different passwords for different accounts & avoid personal number details (DOB, etc.)

- Educate them on guarding customer information
  - “Unfortunately, 64% of small businesses are victims of internal employee theft”

- Install security software
  - Anti-virus, anti-spyware, anti-spam & firewalls are a start...now-a-days you also need business VPN & a software defined perimeter

https://www.perimeter81.com/blog/wi-fi/5-easy-ways-to-keep-your-employees-safe-online/
THE MOST COMMON CAUSE OF A COMPANY DATA BREACH IS EMPLOYEE ERROR

- Train ALL employees on network security
- See what your current employees know
- Create quick reference guides on common types of attacks
- Send out regular emails about the latest threats and news
- Fake a cyber attack, or a phishing attack…

https://www.calyptix.com/top-threats/5-easy-ways-small-it-departments-can-train-employees-on-network-security/
5 PRACTICES TO HELP KEEP YOUR BUSINESS SAFE

- Have an Internet Use Policy
  - The policy should serve as a guideline as to what is acceptable use of company owned technology

- Consider limiting and auditing the number of employees that can install software and access confidential information

- Proactively protect company assets
  - Ensure all of your company computers have an up-to-date anti-virus/antimalware software installed. Companies may also consider implementing a Web Filter to better protect employees from accessing potentially unsafe websites.

- Consider having a secure email solution, not just a spam filter

- Educate! Educate! Educate!
  - Unique & complex passwords for sites, no personal info on an unsecure site, do not click on links in emails/texts/messages from unknown senders

BEST PRACTICES FOR EMPLOYERS OF REMOTE WORKERS

- Require that employees use a non-stored password to connect during each session, especially for VPN access

- Enforce reasonable session time-outs for sensitive programs or applications. A user should not have to reconnect after walking to the kitchen to pour a cup of coffee, but at the same time you cannot trust everyone to always log out for the day

- Limit program/file access to only the areas absolutely needed by that employee

- Reserve the right to terminate employee access at any moment

- Provide services for remote file storage and other tasks; don't rely on individuals to use their personal programs and accounts

https://www.businessnewsdaily.com/9372-secure-home-office.html
BEST PRACTICES FOR REMOTE WORKERS

- Invest in antivirus software
- Don’t allow family members to use your work devices
- Keep your physical workspace secure
- Follow company policies to the letter
- Use a centralized, company-approved storage solution

https://www.businessnewsdaily.com/9372-secure-home-office.html
TOP 10 PERSONAL INTERNET SAFETY RULES

- Keep personal information professional and limited
- Keep your privacy settings on
- Practice safe browsing
- Make sure your internet connection is secure
- Be careful what you download
- Choose strong passwords
- Make online purchases from secure sites
- Be careful what you post
- Be careful who you meet online
- Keep your antivirus program up to date

MIT'S SAFE COMPUTING TIPS LIST

• Patch, Patch, PATCH!
• Install protective software.
• Choose strong passwords.
• Back up on a regular basis.
• Control access to your machine.
• Use email and the internet safely.
• Use secure connections.
• Protect sensitive data.
• Use desktop firewalls.
• Most importantly, stay informed.

https://ist.mit.edu/security/tips
SAMPLE INTERNET USAGE POLICY

Computer, email and internet usage

- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.
- All Internet data that is composed, transmitted and/or received by <company's> computer systems is considered to belong to <company> and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services and technology used to access the Internet are the property of <company> and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.
- All sites and downloads may be monitored and/or blocked by <company> if they are deemed to be harmful and/or not productive to business.
- The installation of software such as instant messaging technology is strictly prohibited.

Unacceptable use of the internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via <company's> email service.
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorization.
SAMPLE INTERNET USAGE POLICY

- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification.

All terms and conditions as stated in this document are applicable to all users of <company's> network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by <company>.

User compliance

I understand and will abide by this Sample Internet Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

__________________________  ____________
Employee signature          Date

COMMENTS? OTHER ISSUES?