LOOKINGGLASS

CYBERSECURITY A-B-C'S
TREAT YOUR BUSINESS LIKE YOUR HOME

2018 has seen
850 reported data breaches and 34 million exposed records.
And that's only in the U.S.[1]

Many breaches, as well as other cyber attacks – ***phishing, ransomware, hacking, etc.*** – could be avoided if basic cyber security precautions were in place.

Secure your organization's network like you would your home network with these cybersecurity best practices.

A. Spot the Phish

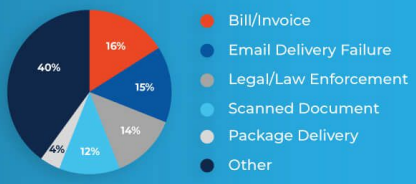
Phishing is one of the **most utilized tactics** to steal personal information – whether via email, website, or social media.

Always think before you click!

30% of phishing messages get opened by targeted users and **12%** of those users click on the malicious attachment or link.

92.4% of malware is delivered via email.[2]

The #1 disguise for distributing malware is via fake invoices.[3]



66% of spear phishing attacks on social media are **being opened by targets.**[4]

In just the first few months of 2018, there was a **46% increase** in the number of phish via website and email.[5]

42% of compromised websites are marked as 'trusted' or 'secure' (HTTPS).[6]

B. Secure Your Passwords

Stolen credentials are the **number one** attack vector for web applications in the past two years.

51% of people don't believe that cybercriminals can figure out their password.

59% of people reuse passwords across multiple accounts.

39% would never change their password if it wasn't required.[7]

Tips for a strong password

Do

- **Use passphrases** instead of words. Incorporate a combination of capital/lower case alpha-numeric and special characters
- Change passwords **frequently**
- **Try password padding** – making your password longer by adding extra characters
- **Multi-factor authentication**
- Employ a **password generator**

Do Not

- **Never** use personal information that can be easily attained by asking common questions
- **Do not** store passwords close to your computer
- **Do not** reuse passwords

C. Patch & Update Systems

Outdated systems and software leave your devices and your organization at risk for targeted attacks by hackers exploiting these vulnerabilities. **Patching vulnerabilities can significantly reduce risk and can stop many hackers completely.**

80% of attacks use vulnerabilities with existing patches.[8]

Best practices for patching:

- **Regularly update** your computer operating system, browser, office applications, and any third party applications.
- When installing software, **pay close attention to the message boxes** before clicking 'OK,' 'Next,' or 'I Agree.'
- Equip computers with **antivirus software and antispyware** – and update regularly.
- **Implement patches** within one week of a release.

Cyber Safety in the Workplace

Keeping your organization safe from cybercrime is the responsiblity of each user. As cyber threats become more sophisticated, employees, executives, and third parties need to stay aware of the newest, as well as prevailing cyber threats. LookingGlass™ offers an award-winning Cyber Safety Awareness Training Program to educate and enable them to proactively identify and shut down threats before they reach the organizations network.

To learn more about our training and for a 14 day free trial, visit www.LookingGlassCyber.com/about-us/contact-us

1 https://www.idtheftcenter.org/wp-content/uploads/2018/09/2018-August-Data-Breach-Package.pdf
2 https://www.verizonenterprise.com/verizon-insights-lab/dbir/
3 https://www.symantec.com/security-center/threat-report
4 https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf
5 https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf
6 https://www.infosecurity-magazine.com/news/42-of-the-webs-top-sites-are/
7 https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/logmein-lastpass-survey-ebook-v8.pdf
8 https://www.computerweekly.com/news/450421649/Security-Think-Tank-Patching-is-vital-and-essentially-a-risk-management-exercise