Staying safe on the Internet

Maxwell Memorial Library

May 16, 2017

1 To start, ...

There are two aspects to online safety: **security** and **privacy**. There is overlap between the two, but security refers to the steps you can undertake to keep your machine, your data, and your identity from being attacked or stolen while privacy focuses on how broad an audience you want for information you share online.

Both of these concepts are important, but different individuals will have greater or lesser desires for privacy. Security needs to be high regardless of how much or little privacy you feel you need.

2 Security

Some of the "common sense" notions that you've acquired about life offline transfers fairly naturally to life online:

- If it sounds too good to be true, it probably is.
- If something seems fishy, it probably is.
- Do business only with reputable and reliable firms.

  How to determine reputation and reliability may require some new skills, though, since you can't rely on cues like that of a brick-and-mortar business's presence in your city for over a century. Customer ratings and reviews are useful.

Seven things security experts do to keep safe online[1]

1. **Install all updates (for both your operating system and your applications)**

   Case in point, the recent ransomware attack — **WanaCrypt0r 2.0** or **WannaCry** — exploits a vulnerability in Windows that Microsoft issued a patch for in March. The malware exploiting it seems to date from mid-April.

   Along these same lines, there was no patch against WannaCry for older Windows systems like XP until just recently. In general, you're safest by upgrading to a new version of software when or before the manufacturer stops supporting the version you're currently using.

[1] Alex Hern, "Seven things security experts do to keep safe online," *The Guardian*, July 27, 2015, accessed May 12, 2017, https://www.theguardian.com/technology/2015/jul/27/security-experts-keep-safe-online-password-manager-seven-things.

2. **Use antivirus software**

   Installing all updates is the first line of defense against attacks, but antivirus and antimalware software is a good part of your whole strategy.

   Windows 8 and later come with **Windows Defender** which is decent and doesn't nag you or share your data like some free, 3rd party antivirus programs do. It doesn't seem to do as well as some 3rd party programs do against some more obscure threats, though. Some free antivirus programs are

   - **Avast** (https://www.avast.com/)
   - **Avira Free Antivirus** (https://www.avira.com/en/antivirus)
   - **Malwarebytes** (https://www.malwarebytes.com/).
     For Mac (https://www.malwarebytes.com/mac/)

   All 3 have both Windows, macOS, and Android versions.

3. **Keep your passwords unique**

   Ideally, all passwords should be strong and unique, but using unique passwords is the more important part of that duet (but see item (4) immediately below).

4. **Use a password manager**

   (a) Keeping track of all the passwords you use taxes the brain. A password manager takes care of that (and many can generate strong, random passwords)

   (b) Microsoft's dissent to this point[2]:

   They recommend using passwords you can remember by splitting the sites you use into 2 classes

   i. Definitely use unique, strong passwords for banking, commerce, other high stakes sites.
   ii. They recommend, however, that you conserve your brainpower for those sites and use and reuse weak passwords for sites that don't hold info you have a high need for security on

   They mistrust password managers because

   i. If the manager only works on one machine, it isn't portable.
   ii. But if the passwords are stored in the cloud, they're vulnerable to hacking.

   (c) Some password managers:

   i. **Dashlane** (https://www.dashlane.com/)
   ii. **LastPass** (https://www.lastpass.com/)

5. **Use two-factor authentication**

   This is where a site requires a temporary security code in addition to your password. The code gets texted to you (there are other ways it can be sent, but this is the most common) and expires after a few minutes.

[2] Alex Hern, "Microsoft tells users to stop using strong passwords everywhere," *The Guardian*, July 16, 2014, accessed May 12, 2017, https://www.theguardian.com/technology/2014/jul/16/microsoft-stop-using-strong-passwords-everywhere.

Two-factor authentication is quite powerful. Even when passwords that aren't quite as strong as recommended or aren't unique, using two-factor authentication might make one safer than having perfect passwords without two-factor authentication.

6. **Look for https in a Website's URL (the address in the address bar)**

   Even sites with organizations you trust can't protect your communication with them if they're using an insecure protocol. **Https** is secure while **http** is not.

7. **Do as I say, not as I do**

   There are various bromides with specific warnings about various online behaviors (for instance, "Never click on links in emails"). Experts, who know how to check whether violating these rules of thumb will be dangerous, will often violate them but only because they know how to do so safely.

3 Privacy

3.1 Those things you might not want everyone to know

A catchphrase on the Internet is "Never share anything online that you wouldn't want your parents/boss/children to possibly see." The idea behind the saying is that (1) nothing vanishes completely on the Internet, (2) it's easy to share anything broadly, and (3) once youve sent or posted something, you no longer control how it's shared.

Like most adages, it has some wisdom in it but shouldn't be taken absolutely: even in the pen-on-paper era, things one wrote could get back to people one might wish they hadn't gotten back to. Nevertheless, the Internet makes communication both more fluid and widespread, so it's worth thinking a bit before sharing, both about the content and the primary audience.

Different people will have different levels of comfort with what they want to risk letting various people see, but the maxim holds in that anything you send in an email or post on Facebook or put in a comment on an online newspaper article or whatever could get seen by potentially anyone.

At the same time, there are measures you can take to make it less likely that what you share will end up in front of people who either mean you harm or who might be upset at seeing it.

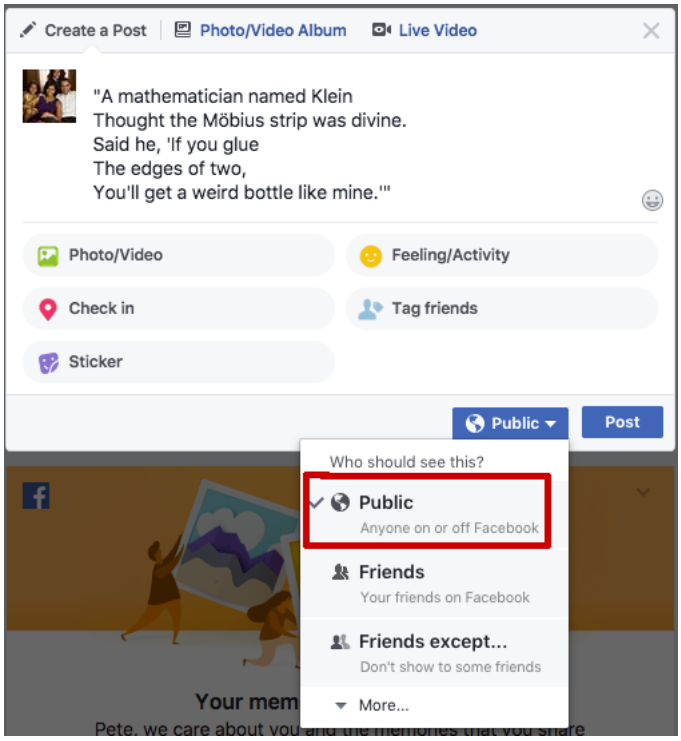
As an example, in Figure 1 I've shown how you can limit the audience for a Facebook post. Notice that I have selected **Public**. This means that anyone on or off Facebook can potentially see this post. If it were something I only wanted my Facebook friends to see, I could have selected **Friends**. If I only wanted a small number of my friends to see it, then under **More ...** I could have chosen **Specific friends** and then given the names of the particular people I wanted to share it with.

However, even with tightly setting the audience, the people you share with might want to share what you write, and then it's out of your control.

3.2 Those things you think it's harmless to share but the reality is a little different: account hacking

"List the first 10 concerts you attended but with 1 of them a lie!"

This was a recent Facebook meme, and like many such memes, it looks innocent and fun but potentially puts you at risk. You see, "What was the first concert you attended?" is a common security question Websites use for password recovery when people forget their passwords.

Figure 1: 

Breaking into systems or individual accounts is extremely difficult. It's much easier to get access when people leave their passwords in the open. Or when they give them away.

4 Appendix

4.1 Strong, unique passwords

From **Stop. Think. Connect.**:

- **Make your password a sentence**

  A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!

- **Unique account, unique password**

  Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

- **Write it down and keep it safe**

  Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer. You can alternatively use a service like a password manager to keep track of your passwords.

- **Lock down your login**

Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

4.2 If you are the victim of a cyber attack

- Immediate actions
  - Check to make sure the software on all of your systems is up-to-date.
  - Run a scan to make sure your system is not infected or acting suspiciously.
  - If you find a problem, disconnect your device from the Internet and perform a full system restore.
- If at home
  - Disconnect your device from the Internet to prevent an attacker or virus from being able to access your system.
  - If you have anti-virus software installed on your device, update the virus definitions and perform a manual scan of your entire system.
  - Install all of the appropriate patches to fix known vulnerabilities.
- If at work
  - If you have access to an IT department, contact them immediately.
  - If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators.
- If at a public place (school, library, etc.)
  - Immediately inform a librarian, teacher, or manager in charge.
  - If they have access to an IT department, contact them immediately.

Other resources

- **Stop. Think. Connect.** (https://stopthinkconnect.org/resources)

  Stop. Think. Connect. is a campaign to raise awareness of issues surrounding safety and security on the Internet. Their Website offers tips on ways to maintain security and privacy.

- **StaySafeOnline.org** (https://staysafeonline.org/)

  StaySafeOnline.org is a site maintained by the National Cyber Security Alliance. It has extensive information on online safety. This includes material for people interested in what they can do to keep themselves, their families, or their businesses safe, and for those who want to teach others how to stay safe.

- **Social networks** (https://staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks)

  How to stay safe in online social networks like Facebook, Twitter, and Google+ and in the comment sections of any online resource.

- **Online shopping** (https://staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping)

  StaySafeOnline.org's page on shopping online.

- **Passwords & securing your accounts** (https://staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securing-your-accounts)

  StaySafeOnline.org's tips for creating passwords that maximize your safety.

- **ID theft, fraud & victims of cybercrime** (https://staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud)

  What to do if your identity is stolen or you otherwise get victimized online.

- **Back it up** (https://staysafeonline.org/stay-safe-online/protect-your-personal-information/back-it-up)

  Keeping backups of important documents and files is a good idea even in a world with no evil. Hard drives fail, people accidentally erase files, and various other glitches happen even in the absense of bad intent.

- Resources for educating your kids about safety online

  - **Rethink cyber safety rules and the "tech talk" with your teens** (https://staysafeonline.org/stay-safe-online/resources/rethink-cyber-safety-rules-and-the-tech-talk-with-your-teens)
  - **Stop. Think. Connect. Tips for parents on raising privacy-savvy kids** (https://staysafeonline.org/stay-safe-online/resources/tips-for-parents-on-raising-privacy-savvy-kids)

- A couple of articles from a recent issue of *The Economist* talking about the Big Picture of computer security at the moment:

  - "The Myth of cyber-security," *The Economist*, April 8, 2017, p. 9.

    "Computers will never be secure. To manage the risks, look to economics rather than technology."

  - "Why everything is hackable," *The Economist*, April 8, 2017, pp. 69–71.

    "Computer security is broken from top to bottom. As the consequences pile up, though, things are starting to improve."