Online Security is More Than Just Passwords

By Denise A. Garofalo
Mount Saint Mary College
Itinerary

• Cybersecurity
• Passwords
• Spam
• Phishing
• Privacy
Cybersecurity and you:
Stop. Think. Connect.
Keep a Clean Machine
Remember to....

- Keep security software current
- Automate software updates
- Protect all devices that connect to the Internet
- Plug & scan
Protect your personal information
Protect your online information

• Secure your accounts
• Make passwords long and strong
• Unique account, unique password
• Write it down and keep it safe
• Own your online presence
Connect With Care

Never access personal or financial information over public wireless networks. Eavesdroppers can observe and change unencrypted communications.
Connect with care

- When in doubt, throw it out
- Get savvy about Wi-Fi hotspots
- Protect your $$
Be wise

• Stay current
• Think before you act
• Back it up
Passwords
How secure are yours?
YOU KNOW YOUR EMAIL PASSWORD?

THAT'S A UNIQUE PASSWORD, RIGHT?

OF COURSE
Supply your password to enter....

CREATE A PASSWORD THAT'S AT LEAST SIX CHARACTERS LONG WITH A MIX OF LETTERS AND NUMBERS.

HOW ABOUT 123?

UH...NO.

IT HAS TO INCLUDE LETTERS AND BE AT LEAST SIX CHARACTERS LONG.

HOW ABOUT ABC?

LETTERS AND NUMBERS AND AT LEAST SIX CHARACTERS LONG!!!

FOURSOME?

GAAA!!!
Create a secure password

• A minimum length: 8 characters
• Include uppercase and lowercase letters
• Use at least one number
• Use at least one special character
Password creation

• **DO NOT USE**
  
  • Birthdates
  
  • Children’s names
  
  • Sports teams
  
  • Words on password blacklists

Password blacklists

• lists of passwords that are too easily cracked
• passwords on these lists are not secure

From https://sdncommunications.com/blog/trust-no-one-is-good-security-advice-but-a-bad-password
Password generators

Sorry, but your password must contain an uppercase letter, a number, a hieroglyph, a feather from a hawk and the blood of a unicorn.

From https://www.smarthomeblog.net/secure-gadgets-iot-botnets/
Password generators

- Random password generator
  https://www.random.org/passwords/
- RoboForm
  https://www.roboform.com/password-generator
- Secure memorable password generator
  https://xkpasswd.net/s/
- Secure password generator
  https://passwordsgenerator.net/
Passphrases instead of passwords

• Take the first letter of each word
  • The quick brown fox jumps over the lazy dog
• Add number and a random character
  • Tqbfjotld
  • 8Tqbfjotld&
Password managers

- DashLane [https://www.dashlane.com/](https://www.dashlane.com/)
- KeePass [https://keepass.info/](https://keepass.info/)
- LastPass [https://lastpass.com/](https://lastpass.com/)
- LogMeOnce [https://www.logmeonce.com/](https://www.logmeonce.com/)
- Roboform [https://www.roboform.com/](https://www.roboform.com/)
- Stickypassword [https://www.sticky password.com/](https://www.sticky password.com/)
- TrueKey [https://www.truekey.com/](https://www.truekey.com/)
How secure is YOUR password?

https://howsecureismypassword.net/
HOW SECURE IS MY PASSWORD?

Your password would be cracked
INSTANTLY
HOW SECURE IS MY PASSWORD?

It would take a computer about

38 BILLION YEARS

to crack your password
Spam
Not just for breakfast anymore
Spam email

- Do **not**
  - respond to spam
  - click to unsubscribe (unless it’s legitimate email, from a store or website you know is real)
  - open any attachment unless it is expected and from someone you know and trust

- If you do reply
  - you confirm for the spammers that it is a live, active email address
  - then they can intensify their efforts at targeting you for their (nefarious) purposes

From http://infostructure.net/news/tag/email-marketing/
Get a handle on spam

• Train your spam filter
• Remember to unsubscribe
• Employ alternative email addresses
• Download third-party extensions and an email client (if you’re not already using one)
• Protect your email address
Phishing
Phishing.....

From https://www.pacific.net/images/phishingcartoon.gif

© Scott Adams, Inc./Dist. by UFS, Inc.
No phishing allowed

• What is phishing?
  • Attack
  • Used to steal user data
    • Login credentials
    • Credit card numbers

• How does it work?
  • Attacker masquerades as a trusted entity
  • Victim is duped into opening an email, instant message, or text message

Foil phishing attacks

- Delete email and text messages that ask you to confirm or provide personal information
- Don’t reply to suspect messages
- Don’t click on links provided in suspect messages
- Prevent images from automatically downloading in emails
- Don’t call numbers from suspect messages
- Instead, call the number on your statement or back of credit card to verify
Steps to avoid phishing attacks

• Use trusted security software (McAvee, AVG, Sophos, etc.)
• Don't email personal or financial information
• Only provide personal or financial info through an organization's website that you type in the URL to reach
• Review credit card and bank account statements for unauthorized charges
• Be cautious about opening attachments and downloading files from emails
Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit [http://www.firstgenericbank.com.account-updateinfo.com](http://www.firstgenericbank.com.account-updateinfo.com).

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank
Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank
Identifying phishing emails

- Company
- Spelling and grammar
- No mention of account information
- Deadlines
- Links

https://www.woodarovebank.com/loginscript/user2.jsp

Common phishing tactics

• Your account has issues
• Personal information issues, including theft
• Confirming recent transactions
PHISHING

INFORMATION

USERNAMES

WEBSITES

COMMUNICATION

VICTIM

NAME

IDENTIFIED

ACCOUNT

ACCOUNT

SUCCESS

ATTACKERS

TECHNOLOGY

THREATS

RECOGNIZED

thumbs up

thumbs down

LOGOS

IDENTITY

THEFT

USER TRAINING

REPORTED

LEGISLATION

SPREADING

MEASURES

UPLOADED

FINANCIAL

PHISHING

LOOK AND FEEL

WEB

COMPUTER

ELECTRONIC

PASSORDS

SITES

SOCIAL NETWORKING

FISHING

PREMIUM

TECHNICAL

DOWNLOADS

EXPERIMENTS

USER TRAINING

IDENTITY THEFT
The email header information of a suspicious message can reveal a forged return address and other details. The New York Times
Dear Employee,

A recent security synchronization for your Mailbox has failed. Kindly proceed to the manual sync portal to synchronize your mailbox immediately.

It is important you proceed to sync your mailbox to prevent functionality issues.

Regards,
Web Central.
Technology Department.
E-post.
Dear Employee,

A recent security synchronization for your Mailbox has failed. Kindly proceed to the manual sync portal to synchronize your mailbox immediately.

-->Manual Sync Service<--

It is important you proceed to sync your mailbox to prevent functionality issues.

Regards

Web Central.
Technology Department.
E-post.
You have two security messages

Kindly sign in to view

Sign In

Lehigh University
Subject: Important Message
Date: Mon, 7 Dec 2015 19:54:41 +0000 (UTC)
From: Lehigh University Alert <slowmotions12@comcast.net>

You have two security messages

Kindly sign in to view

Sign In

Lehigh University
Important: Your Password will expire in 1 day(s)

MyUniversity

to me

12:18 PM (50 minutes ago)

My network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours. Please follow the link below to update your password:
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff
Important: Your Password will expire in 1 day(s)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff
From: University Help Desk [mailto:noreply@its.edu]
Sent: Thursday, May 27, 2010 4:55 PM
Subject: Error Code #984455N.
Importance: High

Attention: Staff/Student,

We are currently carrying out scheduled maintenance, upgrade of our webmail service and we are changing our mailhost server as a result your original password will be reset. We are sorry for any inconvenience caused. To complete and validate your University Webmail Account, upgrade, you must reply to this email immediately and provide the information requested below:

CONFIRM YOUR EMAIL IDENTITY NOW
University Email Address: ...............  
Login ID/ Username: ...............  
Email Password: ...............  
Re-type Password : ...............  

Failure to do this will immediately render your Email Address deactivated from the University Email database. Reply to: (helpdesk01@mail2webmaster.com)

Thank you for being a part of the upgrading exercise.
From: University Help Desk [mailto:noreply@its.edu]
Sent: Thursday, May 27, 2010 4:55 PM
Subject: Error Code #984455N.
Importance: High

Attention: Staff/Student,

We are currently carrying out scheduled maintenance, upgrade of our webmail service and we are changing our mailhost server as a result your original password will be reset. We are sorry for any inconvenience caused. To complete and validate your University Webmail Account, upgrade, you must reply to this email immediately and provide the information requested below:

CONFIRM YOUR EMAIL IDENTITY NOW
University Email Address: .............
Login ID/ Username: ..............
Email Password: .............
Re-type Password: .............

Failure to do this will immediately render your Email Address deactivated from the University Email database. Reply to:

(helpdesk01@mail2webmaster.com)

Thank you for being a part of the upgrading exercise.
Images within email messages

- Known as web beacons
- Can be malicious
  - Secretly send a message back to the sender
- Information sent back is used to locate active email addresses
- Can also contain harmful codes to bypass spam filters
- Prevent web beacons from doing harm
  - Adjust email settings to prevent pictures from downloading until you've had a chance to review the message
Privacy
NEARLY
90%
OF ALL PAGE LOADS CONTAIN TRACKERS

"The Tracker Tax" - Ghostery report 2018
AVERAGE PAGE LOAD TIME
WITH vs. WITHOUT TRACKERS

No trackers blocked
19.3

More than 2x slower when no trackers blocked

All trackers blocked
8.6
SECONDS TO LOAD A WEBSITE
WITH vs. WITHOUT TRACKERS

- cracked.com
  - All trackers blocked: 13.3
  - No trackers blocked: 126.5

- si.com
  - All trackers blocked: 9.3
  - No trackers blocked: 120.7

- chron.com
  - All trackers blocked: 9.9
  - No trackers blocked: 97.4

- nypost.com
  - All trackers blocked: 8.3
  - No trackers blocked: 96.9

- pcmag.com
  - All trackers blocked: 12.9
  - No trackers blocked: 88.1
Consider changing your privacy settings on social media websites and apps.
Consider disabling location-tagging on your phone and in the apps you use.
Consider scrubbing your photos you add to social media.
Social media safety

• Be selective with friend requests
• Click links with caution
• Be careful about what you share
If it's on the Internet, it isn't private.
Tips to protect your privacy on the Internet

• Tape over all your webcams (when not in use)
• Install tracker blockers on your browser
• Use ad blockers
• Choose a private search engine as your default
• Select private browser sessions
• Use different browsers for different things
• Disable location services
• Say “no” to always on voice assistants
From http://2.bp.blogspot.com/-FYesyv2S5UUX-HOvVWwI/AAAAAAAABBo/SpNnqoICwal/s1600/cartoon_nicer_than_facebook.jpg

OF COURSE, I EXPECT ALL OF THIS TO REMAIN STRICTLY PRIVATE!

NAME... AGE... GENDER... HEIGHT... WEIGHT...
SSN... NET WORTH...
MARITAL STATUS...
PET PEEVES...
WORST FEARS...
SEXUAL FANTASIES...
MEDICAL HISTORY...

Mike Keefe, The Denver Post

www.caglecartoons.com
PUBLIC OPINION & KNOWLEDGE ON PRIVACY

12 OUT OF 15
PEOPLE ACCEPT THAT DISCLOSURE OF PERSONAL INFORMATION IS
‘A FACT OF MODERN LIFE’

40% OF 25-34 YEAR OLDS REGARD THEIR PERSONAL INFORMATION AS A COMMODITY TO BE TRADED WITH COMPANIES IN EXCHANGE FOR FREE SERVICES OR BETTER BENEFITS. (35% OF OTHER AGE GROUPS THINK THE SAME.)

60% OF US ADULTS BELIEVE COMPANIES SHOULD ONLY BE ABLE TO TRACK THEIR ONLINE ACTIVITIES AFTER THEY HAVE SPECIFICALLY GIVEN PERMISSION TO DO SO.

45% OF US ADULTS FEEL THAT THEY HAVE LITTLE OR NO CONTROL OVER THE PERSONAL INFORMATION COMPANIES GATHER WHILE THEY ARE ONLINE.

40% OF US ADULTS SAY THEY UNDERSTAND HOW TO PROTECT THEIR ONLINE PRIVACY.

32% OF US ADULTS ALWAYS CONSIDER A COMPANY’S PRIVACY POLICIES WHEN CHOOSING WHICH WEBSITES TO VISIT OR ONLINE SERVICES TO USE.

From University of California at Riverdale
Consider the following
Friends of Friends

Whoa, Mr. Anthony liked my picture! If he can see that, I'd better be careful what I post.
Think Twice

Why does this free music site want my credit card information? That's weird...
It’s okay if I post this, because it’s private.

Have you read the privacy policy for that site? It’s not what you think it is.

From https://www.pixton.com/schools/teacher-resources/lesson-plans/privacy-online
RETHINKING PRIVACY IN THE AGE OF SOCIAL MEDIA...

DID YOU HAVE ANY OTHER QUESTIONS FOR ME?

YEAH...I WAS JUST WONDERING WHY YOU'D WANT A TATTOO IN SUCH AN UNUSUAL PLACE...
PROTECT YOUR PRIVACY ON YOUR MOBILE DEVICE

- Avoid apps that leak your information
- Use anti-virus software
- Erase all apps before you recycle
- Beware untrusted apps
- Clear out unused apps
- Protect your device
Resources

- Adams, S. (n.d.). *Dilbert* [Cartoon].
- Chrome add-on: Collusion at https://github.com/toolness/collusion
Resources


• Murphy, K. (2014, October 04). *We want privacy, but can’t stop sharing.* Retrieved from https://www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html?mcubz=1&_r=0


Review

- Cybersecurity
- Passwords
- Spam
- Phishing
- Privacy