Information Security Tips You Can Use Now

Brian Anderson
Security Training & Communications Manager
Office of Information Security

Why Information Security Training?

Information Security Training and Communications

- The primary objective of our security training and communications program is to promote security-driven decisions and educate members of the BYU community on our shared responsibility to help protect our information and information assets. Information security should become a part of our cultural DNA. Ultimately, the goal is to **develop security-aware employees and students**.

- **Security culture:** What happens with security when people are left to their own devices.

Why is topic this important?

It's real and it can happen to you.

It's not, "if" but 'when'

It disturbs and interrupts our life goals and activities

Costs: Time, Money, Reputation, Security

Objectives

- “Be Wise → Be Alert”
- By the end of the session you will walk away with tips that will help you secure your technology and protect your information.
- You’ll be able to apply these tips at work and at home.

Know the Terrain

YOU ARE A TARGET

SANS SECURITY AWARENESS

You may not realize it, but you are a target for cyber criminals. Your computer, mobile devices, accounts and your information have tremendous value. Check out the different methods a criminal could use your information against you to make money or commit other crimes.

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name
- Your UPS or FedEx accounts, where they ship stolen goods in your name

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list
- All of your personal or work email

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information
- Your tax records and past filings
- Your financial investments and retirement plans

Extortion

Once hacked, cyber criminals can take over by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures
- Encrypting all the data on your computer and demanding payment to decrypt it
- Tracking all websites you visit and threatening to publish them

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people
- Launching Denial of Service attacks

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account
- Your email accounts
- Your Skype or other IM accounts

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- Hosting phishing websites to steal other people's usernames and passwords
- Hosting attacking tools that will hack people's computers
- Distributing child pornography, pirated videos or stolen music

Fortunately, by taking a few simple steps, you can protect your organization and your family. To learn more, visit: **sans.org/security-awareness**.
This poster was developed from security awareness expert **Brian Krebs**. Learn more about cyber criminals at: **krebsonsecurity.com**.

Our University

- Academic Records and Grades
- Personal Identifiable Information (PII)
- Financial Aid Information
- Bank Information
- Credit Card Information
- Payroll
- Department Research Data
- Accounts Payable, Vendors

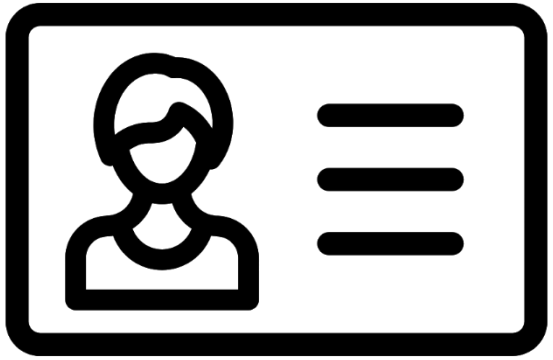
Why do people do this?

- $608 billion – 2018 estimate
- Technology Revolution – easily to be seen as data points and not people/human beings.
- It's a numbers game – only a small percentage need to be exploited
- Cybercrime as a service
- Sold on the dark web

Remember: You are a target. BYU is a target.

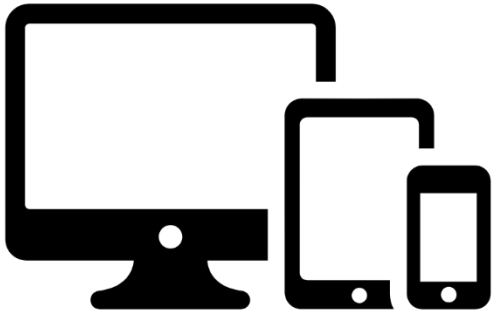
How do you protect yourself?

Protect your email



Protect your identity

Protect your access



Protect your device

Protect your email

What is phishing?

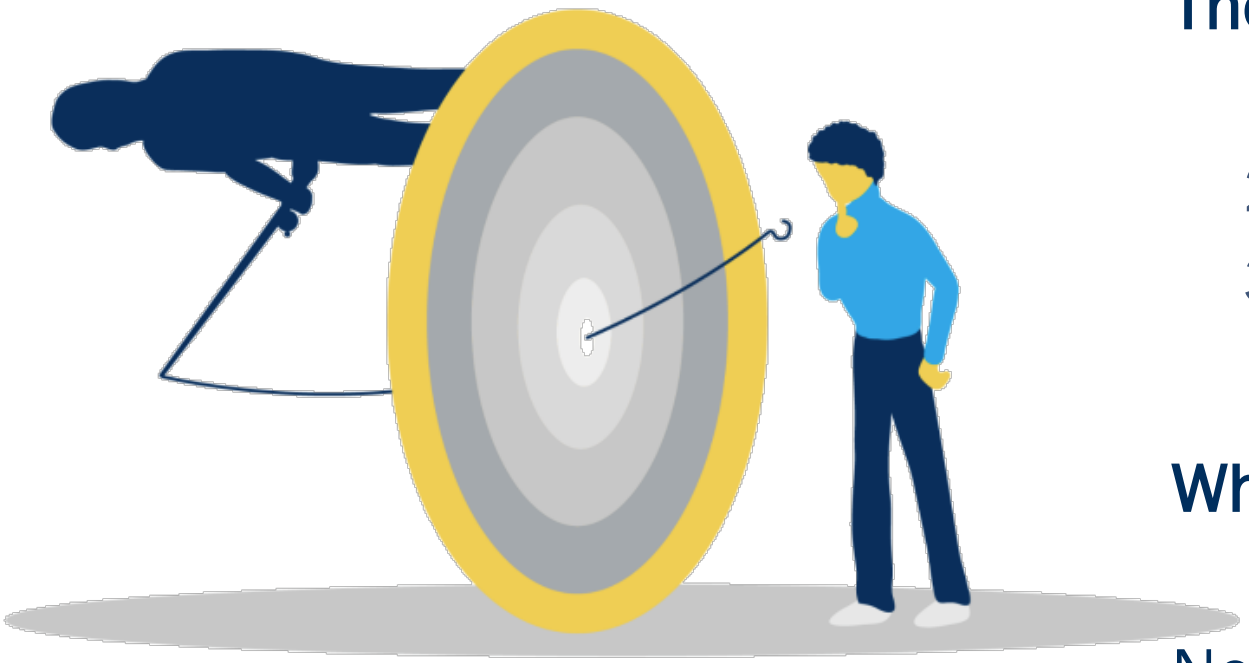
General Definition

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone with the intent to **lure individuals** into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss. (phishing.org)

Protect your email

What do they want?



They want:

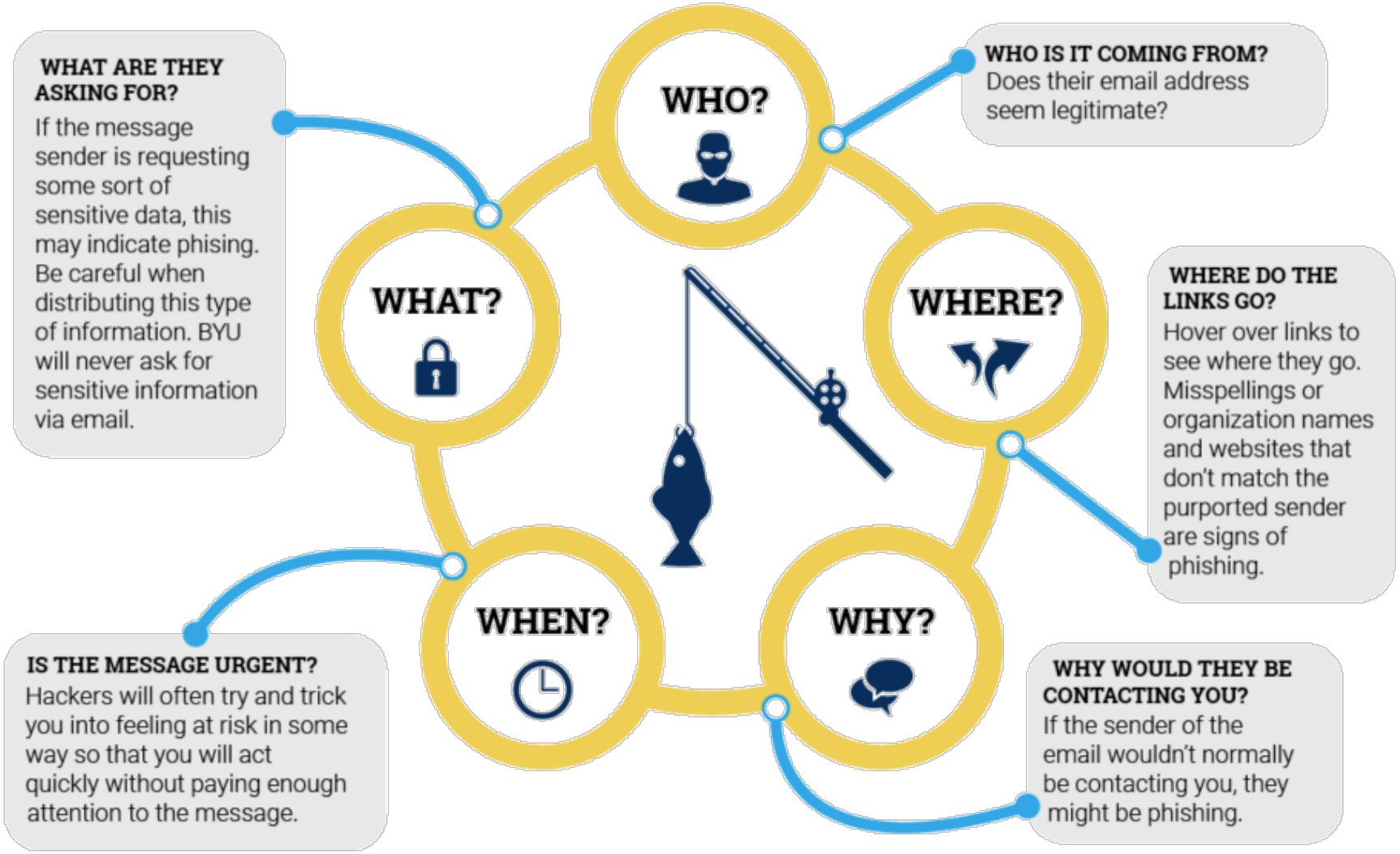
1. Your information – Credential Hunting
2. Your money - Scam
3. Control of your computer - Malware

What can we do?

Not give them these things.
(Sometimes seems easier said than done).

Protect your email

Tip: Ask Questions



WHAT ARE THEY ASKING FOR?
If the message sender is requesting some sort of sensitive data, this may indicate phising. Be careful when distributing this type of information. BYU will never ask for sensitive information via email.

WHO IS IT COMING FROM?
Does their email address seem legitimate?

WHERE DO THE LINKS GO?
Hover over links to see where they go. Misspellings or organization names and websites that don't match the purported sender are signs of phishing.

IS THE MESSAGE URGENT?
Hackers will often try and trick you into feeling at risk in some way so that you will act quickly without paying enough attention to the message.

WHY WOULD THEY BE CONTACTING YOU?
If the sender of the email wouldn't normally be contacting you, they might be phishing.

Signs of Possible Phishing

- Poor grammar, spelling, or sentence structure
- Message is missing your name
- Sender's name doesn't match the email or the sender's organization
- Urgent, required, mandatory, or other emotional trigger
- Asking for password or other sensitive data
- Pretends to be IT or someone in authority
- Too good to be true
- Asking you to do something outside of policy or protocol
- You don't do business with that company

Protect your email

What to do?

- Ask questions
- Hover over links
- Double-check sender's email address
- Check grammar
- Don't open attachments
- Call the person or reach out securely
- Forward to abuse@byu.edu

Protect your email

Phishing Example

Protect your email

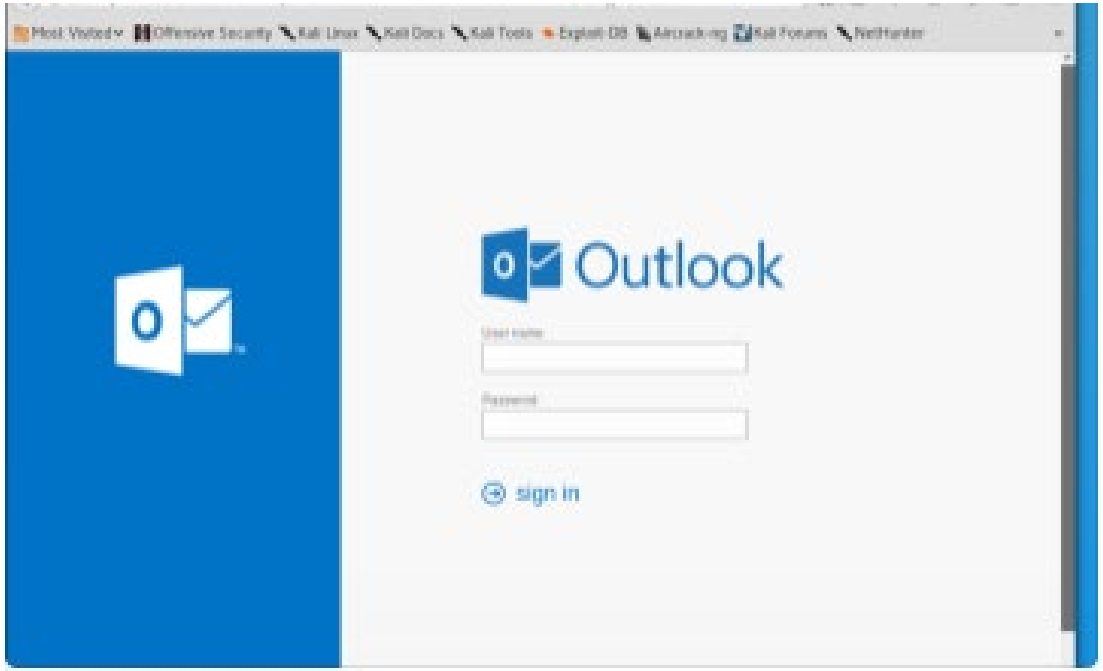
Credential Hunting

From: Sadri, Mahmoud MSadri@twu.edu
Sent: Thursday, December 6, 2018 11:25 AM
To: mail@mail.com
Subject: You have been sent a file using Dropbox

Dear Byu.edu user

You have been sent a file (invoice.pdf) using Dropbox

View Here



Protect your email

Phony Message from President

Malware Alert Text.txt
502 bytes

From: Sis Law <sis@cedarland-homes.com>
Date: August 27, 2019 at 1:06:41 PM MDT
To: Undisclosed recipients:;
Subject: BYU Re-Evaluated and Up to Date Information Security Policy For All Employees

Message From President Kevin J Worthen

Dear Colleagues:

We aim to provide guidance and align our behaviors as we make great decisions that impact our daily operations. We rely on our values and this code as guidelines, as a breach of the Policy may result in disciplinary action against the Employee concerned.

All employees, including all individuals on full-time or part-time employment with the institution, are required to go through the guidelines attached in this email. We all must adhere to these guidelines so you will be helping to ensure the future success of this great institution.

Thank you for your ongoing commitment to delivering a better and reliable service.

Sincerely

Kevin J Worthen
President
Brigham Young University
Provo, Utah, United States
P: 801-422-4636

Protect your email

Gift Card

Things we can do:

- Check out the sender's address.
- Is this a request that sounds like the person would make?
- How can I confirm it's the person?
- Contact the person via another communication channel (at a known email or via phone).

- Report to abuse@byu.edu.

What is Social Engineering

Social engineering is a broad term used to describe a range of techniques to trick people into giving fraudsters what they want. Often the focus is on taking advantage of the social norms and avenues of our community.

Types of social engineering include:

- Fake social media profiles
- Piggybacking into secure locations
- Using physical technology (USB, Gift of charging cord)
- Vishing (voice or phone phishing)

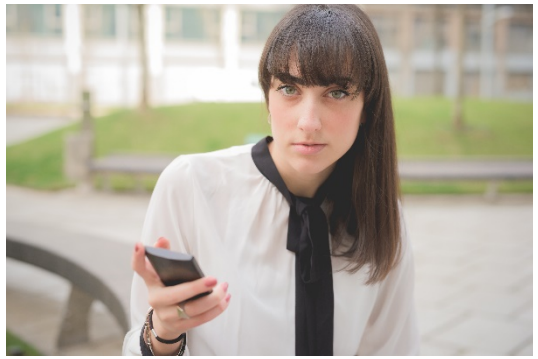
Vishing Example

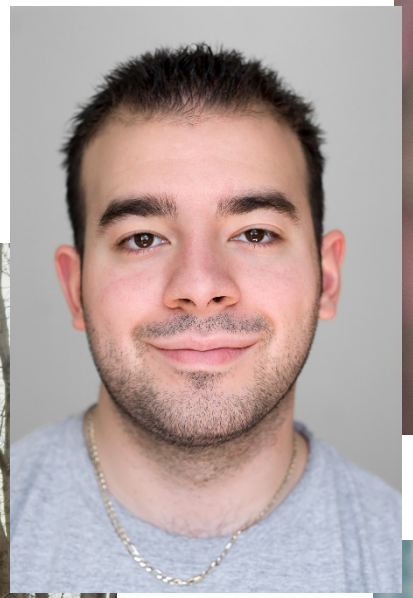
Social Media & Social Engineering

Own your presence

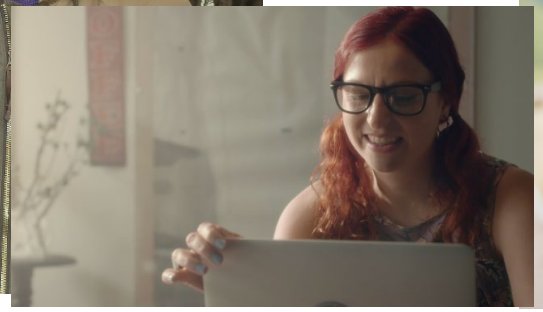
- What can I find out about you?
- What do you share?
- Kids names?
- Schools?
- Employment? Coworkers?
- Hobbies?
- Vacation? Travel?

Who's the 'Social Engineer'?









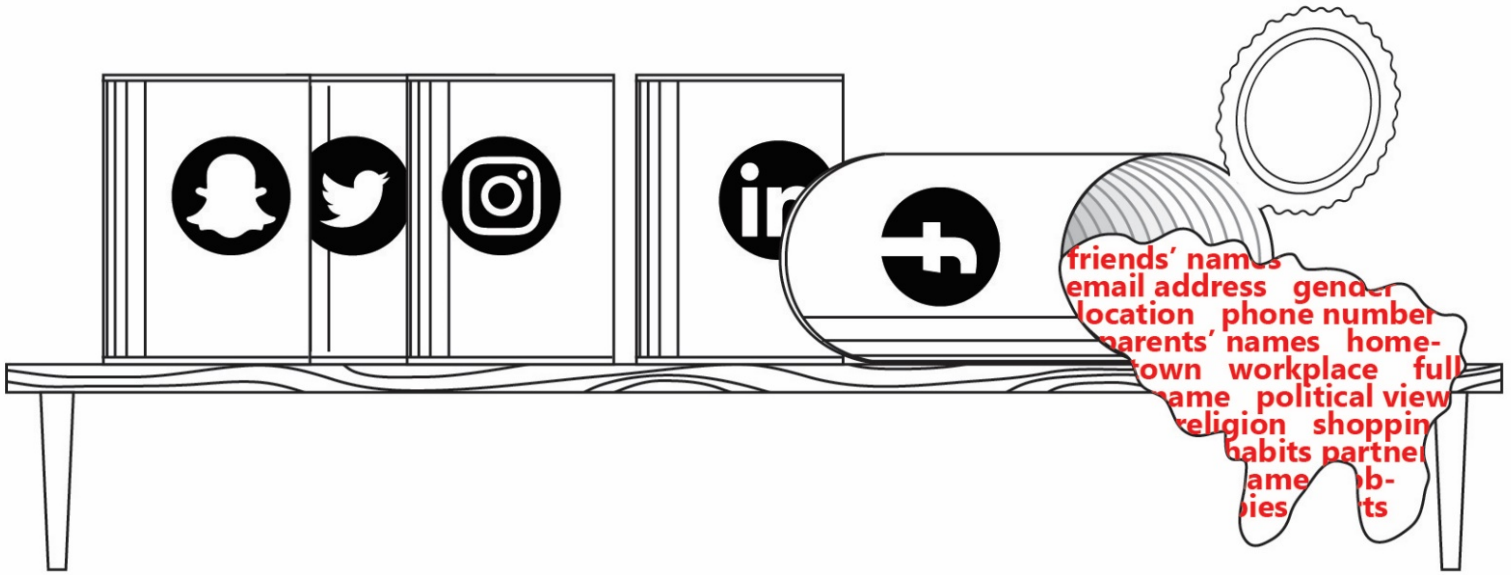

It’s what I do...

What can you do?

Own your presence

- Take an inventory of your ‘friends’. How many, how close, how to you know them, and how are you connected to them?
- Would you pick up the phone and call each of them?
- Would I share this with a stranger? Don’t be afraid to unfriend.
- Manage your privacy settings:
  - Facebook
  - Twitter
  - Instagram
  - Linked-In

What can you do?



keep it canned. take control of your privacy settings.

Password Management

Practice Good Hygiene (routines and maintenance)

- Do not share
- Create and use strong passwords
- A separate password for each system/account
- Use DUO
- Use Password Manager

Do Not Share It!

Passwords


choose your passwords
like you're choosing cougartails*
*just no sharing

Top 25 Passwords (2018)

123456
password
123456789
12345678
12345

111111
1234567
sunshine
qwerty
iloveyou

princess
Admin
Welcome
666666
Abc123

football
123123
monkey
654321
!@#$%^&*

charlie
aa123456
donald
password1
qwerty123

Passwords at byu

Anything with:

- Cosmo
- Cosmocougar
- Cougar
- Byu
- Cougars
- Department name

Strong Passwords

- Strength
  - Passphrases
  - Longer (alphabet only, shorter more characters)
  - No family names, pet names or birthdates
  - Easy to for you to remember but hard for others to guess
  - No common passwords!
  - Do not use default passwords (especially for administrative systems and credentials)

Resources – password checker only as a tool! https://howsecureismypassword.net

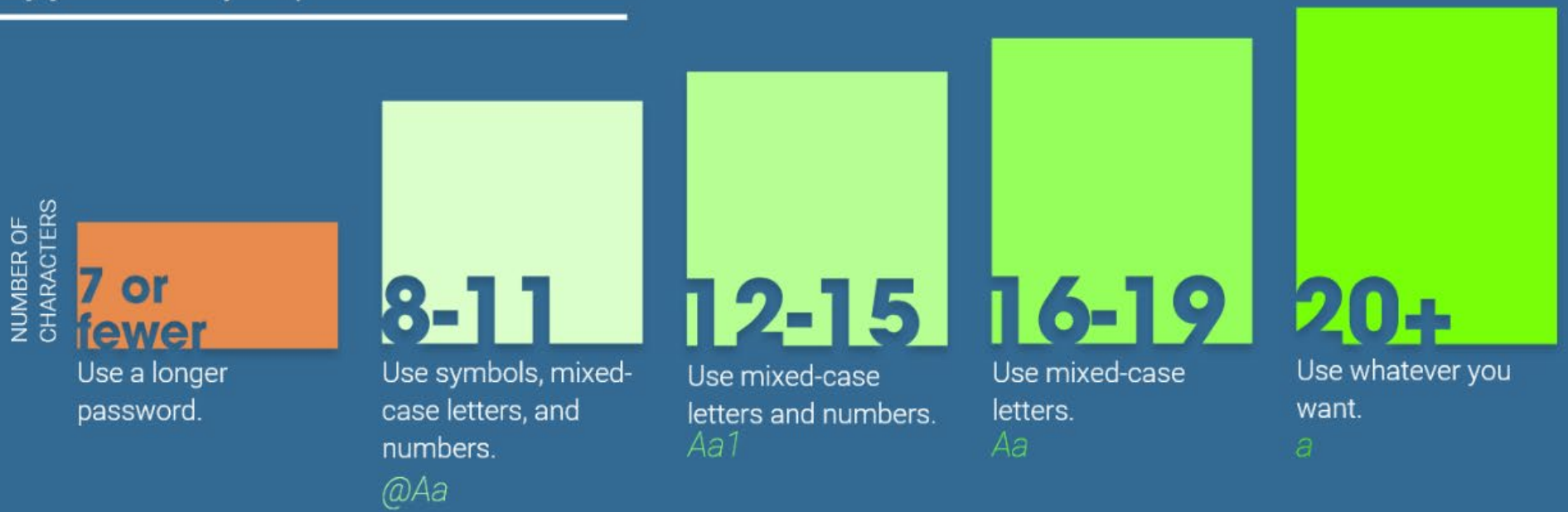
GUIDELINES for CREATING STRONG PASSWORDS

BYU OFFICE OF INFORMATION SECURITY

Strong passwords aren't hard to make.

Here's how to give yours a boost.

The shorter you make your passwords, the more complex they need to be to stay strong. Use these guidelines to help you decide how much variety you need in your passwords.



Passphrase

Use DUO

DUO MOBILE

A wingman for the digital age

Multifactor authentication is another crucial defense against hacking and should be used whenever possible. Multifactor authentication, or two-step verification, requires authentication through a second device. Duo is a two-step verification service that BYU requires for most of its websites. Like other multifactor authentication services, Duo strengthens security and protects against hackers.

Click here to enroll in Duo Mobile

1. Open Duo
2. Click "Enroll"
3. Fill in your BYU username and password
4. Click "Start Setup"
5. Add your device and follow the instructions for installing Duo

Protect your device

- Safe surfing (look for ‘https:’ - secure certification)
- Clean your inbox
- Create backups on cloud (i.e. Box) or hard drive
- Update your software
- Use anti-virus, we use Sophos
- Lock your screen when leaving your desk
- Don’t use public Wi-Fi for transactions
- Don’t leave phone/device in public area (even if just for a few minutes)

SECURITY INCIDENTS

After taking all available security precautions, it's important to continue being vigilant in monitoring your accounts. Regularly check your personal financial accounts, school accounts such as MyBYU and My Financial Center, and social media and entertainment accounts for suspicious activity.

If you suspect or know that an incident has occurred, follow these steps:

1. Immediately contact the OIT Service Desk. Do NOT try to remediate the incident on your own.
2. Report the incident to your management chain.
3. Disconnect the computer or device from the network to stop/minimize any potential external hack or loss of data.
4. Keep the device on and running-do NOT turn off or restart your device. This will help preserve the current state of the system.
5. Do not continue to use the device.
6. Cooperate with any analysis or investigation that may follow.

Remember: Information security incidents are part of our current environment and can happen to anyone. If you are unsure whether an event is a security incident, it is best to reach out and report the event.

In the case of physical threats or theft of equipment, report the incident to the police. If a university device or a personal device storing sensitive university information is involved, notify the OIT service desk as well.
On-campus Police: (801) 422-2222
OIT Service Desk: (801) 422-4000

RESOURCES

- Security Awareness Media Kits
- Infosec.byu.edu
- Besafe.byu.edu
- Staysafeonline.org
- ftc.gov
- stopthinkconnect.org
- Department CSR

Brian Anderson
Briank_Anderson@byu.edu
801-422-0362

CES Security Operations Center
cessoc@byu.edu
801-422-7788

Be Wise, Be Alert.

This is in our power.

We can do this.

Secure **Y**ourself, Secure the **Y**.