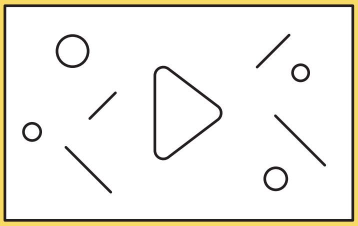
SECURITY AWARENESS KITS

In an effort to educate the BYU community about information security, we've created an expanding collection of media that BYU faculty and staff can easily implement into everyday training situations. These can be distributed and used freely.

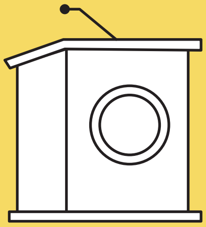
POSTERS

Detailed posters that break down key elements of information security individually.



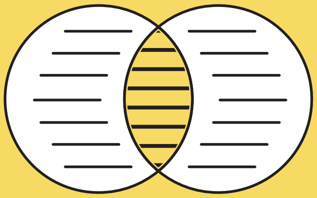
VIDEOS*

General–audience videos explaining and demonstrating important information security principles.



TALKING POINTS*

Guides for how to discuss information security relevantly and effectively.



GRAPHICS*

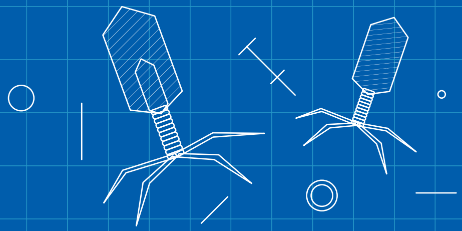
Infographics and images that can be used in presentations and emails to support messages about information security.

questions? contact infosectraining@byu.edu

*coming soon

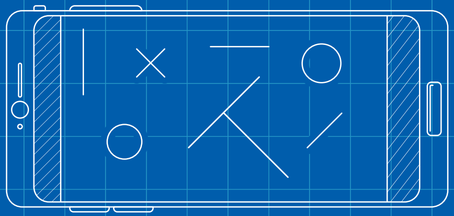
BYU | OFFICE OF INFORMATION SECURITY

INFORMATION SECURITY MYTHS AND FACTS



"If I've got antivirus software, I'm safe."

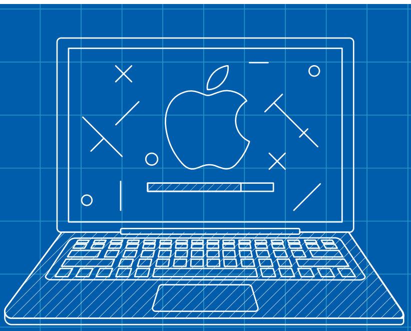
Antivirus software can detect and fight malware once it's been downloaded, but it can't stop the attack from happening. What's more, hackers actively develop viruses that are built to sneak past antivirus software.



"My phone is safer than my computer because it can't get hacked."

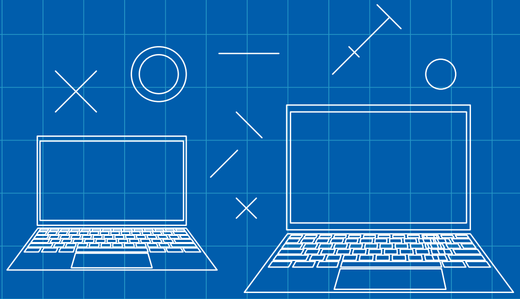
Many of the cyber security breaches you hear about involve computers, but your smartphone needs protection too! It should be equipped with antivirus software and the latest application updates. Be aware that phishing can happen through links in text messages, too.

BYU | OFFICE OF INFORMATION SECURITY



"I have a Mac, and they don't get viruses."

Unfortunately, no computer is 100% safe on its own; plenty of hackers have successfully attacked Macs in the past. Yes, most viruses target Windows, but that doesn't exempt Apple-lovers from using safe digital habits.



"Nobody wants to hack me, I'm not that important."

The truth is, hackers don't discriminate. It doesn't matter how old, wealthy, or tech-saavy you are – if you have any kind of internet presence, you're a target for malware and identity theft.

"BYU's tech people are in charge of stopping viruses."

BYU's Information Security team can fight cyberattacks when they occur, but they're usually playing defense. If we want to stop cyberattacks from happening, we have to be smart in our own computer use.

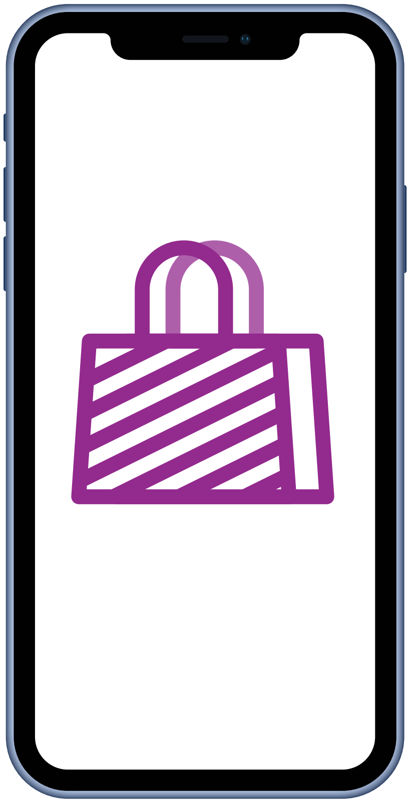
The weak link.

Phones are an easy gateway for hackers to get
to your information, so...
Use secure WiFi.
Back up your data.
Mind which passwords autofill.
Unlock with your fingerprint or face.

Breathe easy.

BYU | OFFICE OF INFORMATION SECURITY

Shop around...
but not *too* around.



Only get your apps from Google Play or the App Store. Do a little research first so you don't download something malicious by accident.

BYU | OFFICE OF INFORMATION SECURITY

O Be WiseFi.

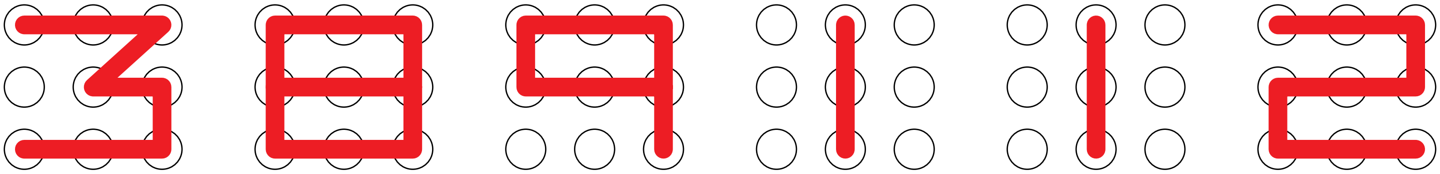
Make sure you're on a secure network.
If you have to use public WiFi, be
aware that your data might not be
hidden from others.

BYU | OFFICE OF INFORMATION SECURITY

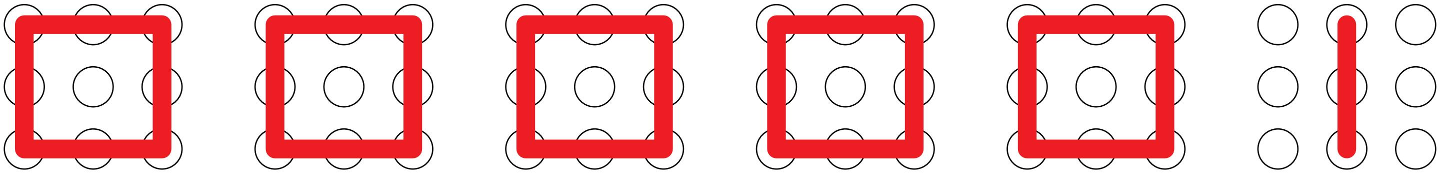
Have cake & eat it too. Or just have two cakes.

Use cloud apps to regularly back up your photos, music, and files to online folders. Having duplicates will save you pain if your phone gets lost, stolen, or hacked.

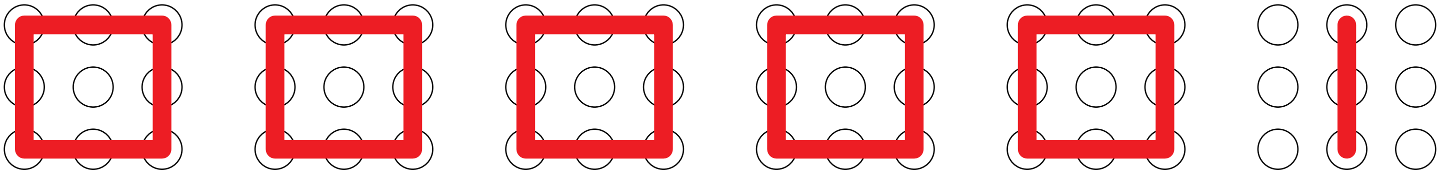
BYU | OFFICE OF INFORMATION SECURITY



That's how many possible unlock patterns there are.



That's how many times most people need to see your pattern to copy it.



That's how many people have your fingerprint and face.

Unlock wisely.

BYU | OFFICE OF INFORMATION SECURITY

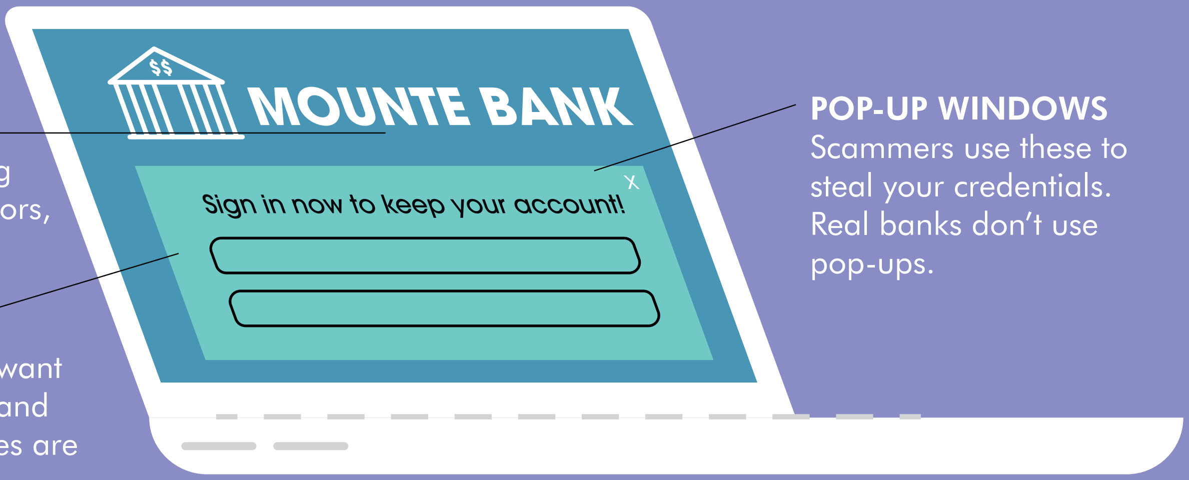
ONLINE SCAMS of the WORLD

FAKE BANK SITES

Phishing emails that say they come from a bank usually include links that will take you to a spoofed copy of the real bank's website. If you click, you may end up divulging personal and financial info.

WHAT ARE THE SIGNS?

Spoofed bank sites are designed to look as identical to their legitimate counterparts as possible, but certain site elements might help tip you off.



POOR DESIGN
Beware of spelling and grammar errors, or design flaws

URGENCY
Scammers don't want you to take time and consider. Real sites are much kinder.

POP-UP WINDOWS
Scammers use these to steal your credentials. Real banks don't use pop-ups.

WHAT CAN YOU DO?

Never click on links in emails that appear to come from your bank.

Use a browser that has a built-in **pop-up blocker.**

Always type the link manually or use your existing autofilled web address. Use a trusted search engine like Google.

If something important really needs your attention, you will be alerted about it by your bank **when you access your account normally.**

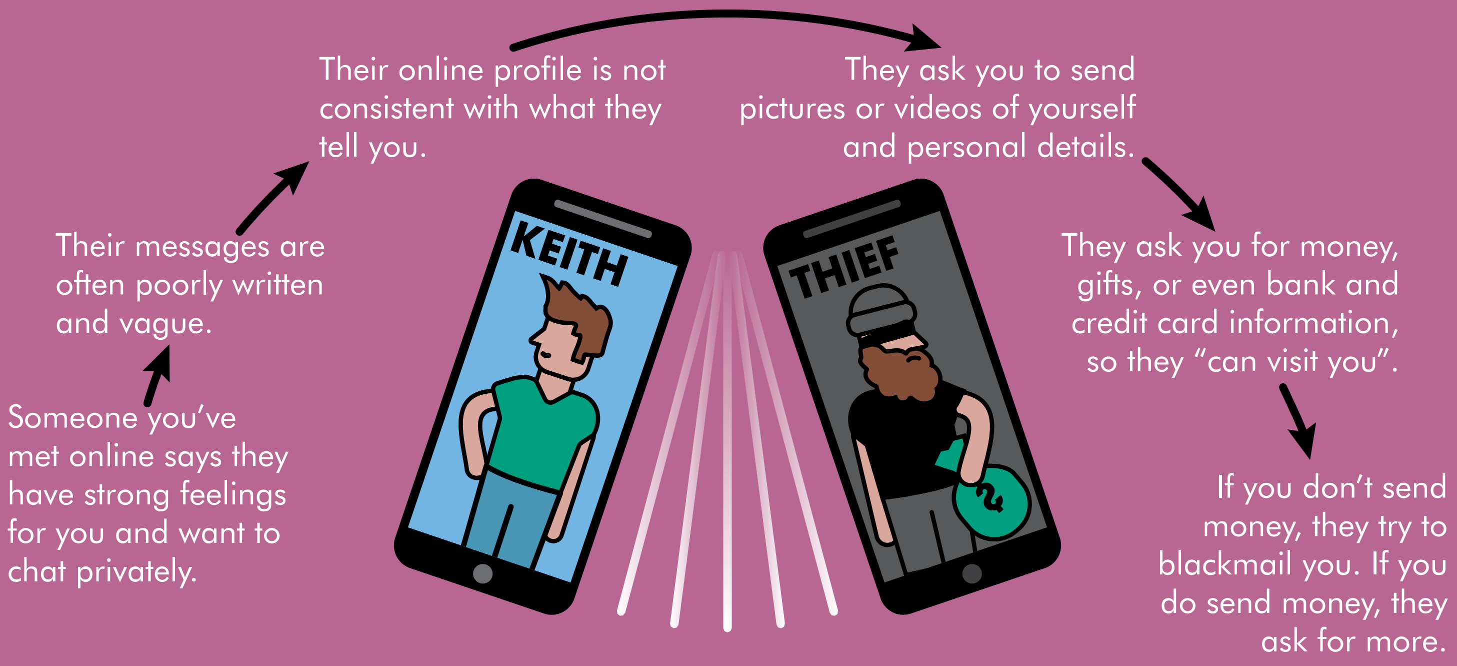
BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

BAD ROMANCE

Dating is hard enough without getting roped in by a fraud. Whether it's on a dating app, a matching site, or social media, look out for scammers – even if they're a perfect match.

WHAT ARE THE SIGNS?



Someone you've met online says they have strong feelings for you and want to chat privately.

Their messages are often poorly written and vague.

Their online profile is not consistent with what they tell you.

They ask you to send pictures or videos of yourself and personal details.

They ask you for money, gifts, or even bank and credit card information, so they "can visit you".

If you don't send money, they try to blackmail you. If you do send money, they ask for more.

WHAT CAN YOU DO?

- Ask to meet in person, in a public and safe place
- Be very careful about what personal information you share on social network and dating sites
- Never send money, credit card details, online account details, or copies of personal documents
- Stay vigilant - even reputable sites have scammers
- Go slow and ask questions
- Research the person's photo and profile to see if the material has been used elsewhere
- Be alert to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working
- Don't share any compromising material that could be used to blackmail you
- If you agree to meet in person, tell family and friends where you are going
- Don't transfer money for someone else: money laundering is a criminal offense

IF YOU ARE A VICTIM

- Don't feel embarrassed!
- Stop all contact immediately
- File a complaint with the police
- Keep all your old chats with them, if possible
- Report the scammer to the site where you met
- If you gave account details, contact your bank

BYU | OFFICE OF INFORMATION SECURITY

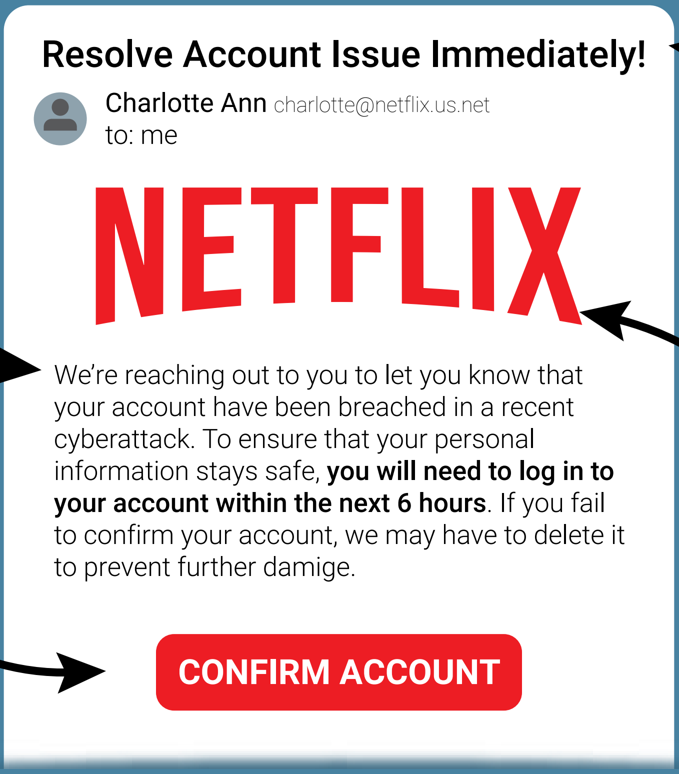
ONLINE SCAMS of the WORLD

PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receiver into sharing their personal, financial, or security-related information. Phishing emails typically:

...appear **nearly identical** to the types of emails the real organization would send

...ask you to **download** an attached file or click on a link



Resolve Account Issue Immediately!

Charlotte Ann charlotte@netflix.us.net
to: me

We're reaching out to you to let you know that your account have been breached in a recent cyberattack. To ensure that your personal information stays safe, **you will need to log in to your account within the next 6 hours**. If you fail to confirm your account, we may have to delete it to prevent further damige.

...use language that transmits **a sense of urgency**

...**replicate the logos**, layout, and tone of real emails

Cybercriminals rely on impatience or fear to get their targets to respond blindly. Watch out when using a mobile device, as it's harder to spot phishing on a phone or tablet.

WHAT CAN YOU DO?

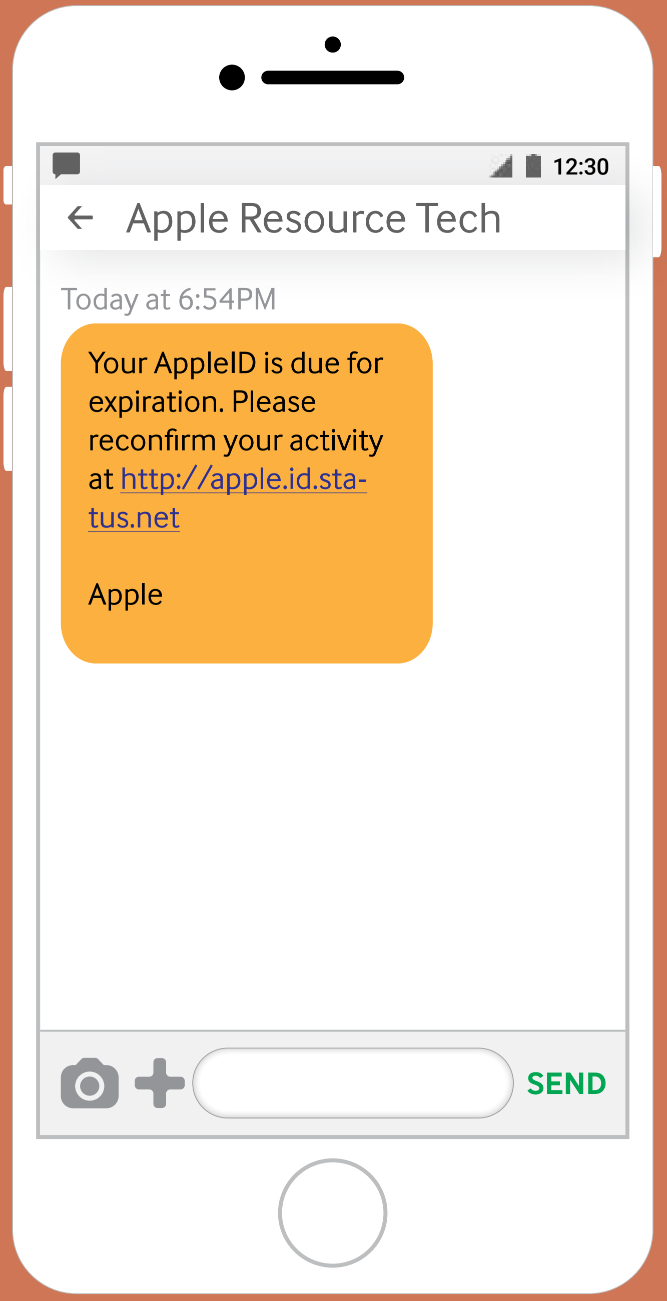
- *Keep your software updated, including your browser, antivirus, & operating system*
- *Be especially vigilant if an email requests sensitive information from you*
- *Look at the email address closely: compare the address with previous messages*
- *Check for bad spelling and grammar*
- *Don't reply to a suspicious email*
- *Don't click on links or download attachments; instead type the address by hand*
- *When in doubt, double check with the organization's website or give them a call*

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

SMISHING

Smishing is phishing – using fraudulent emails to "fish" for victims' personal data – applied to the more intimate world of SMS text messaging.



Apple Resource Tech

Today at 6:54PM

Your AppleID is due for expiration. Please reconfirm your activity at http://apple.id.status.net

Apple

HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account.

But the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

A cleverly designed fake website or believable phone call can fool even the tech-saavy into accidentally giving away personal information, making them vulnerable to cyberattacks.

WHAT CAN YOU DO?

→ Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender using known contact information.

→ Don't be rushed. Take your time and make the appropriate checks before responding.

→ Never respond to a text message that requests your PIN or your online banking password or any other security credentials.

→ If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

VISHING

Vishing is short for "voice phishing", and refers to phonecall scams, including robocalls and any other fraudulent activity that might trick someone into divulging personal information.

WHAT CAN YOU DO?

- → Beware of unsolicited telephone calls.
- → Remember that modern scammers can make robocalls from numbers similar to yours. Inspect the caller ID first, but remember that called ID can be spoofed. If you don't know them or weren't expecting the call, send the call to voicemail.
- → Take the caller's number and advise them that you will call them back.
- → In order to validate their identity, look up the organization's phone number and contact them directly.
- → Don't validate the caller using the phone number they have given you (this could be a fake or spoofed number).
- → Fraudsters can find your basic information online (e.g. social media). Don't assume a caller is genuine just because they have such details.
- → Don't share your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- → Don't transfer money to another account on their request. Your bank will never ask you to do so.

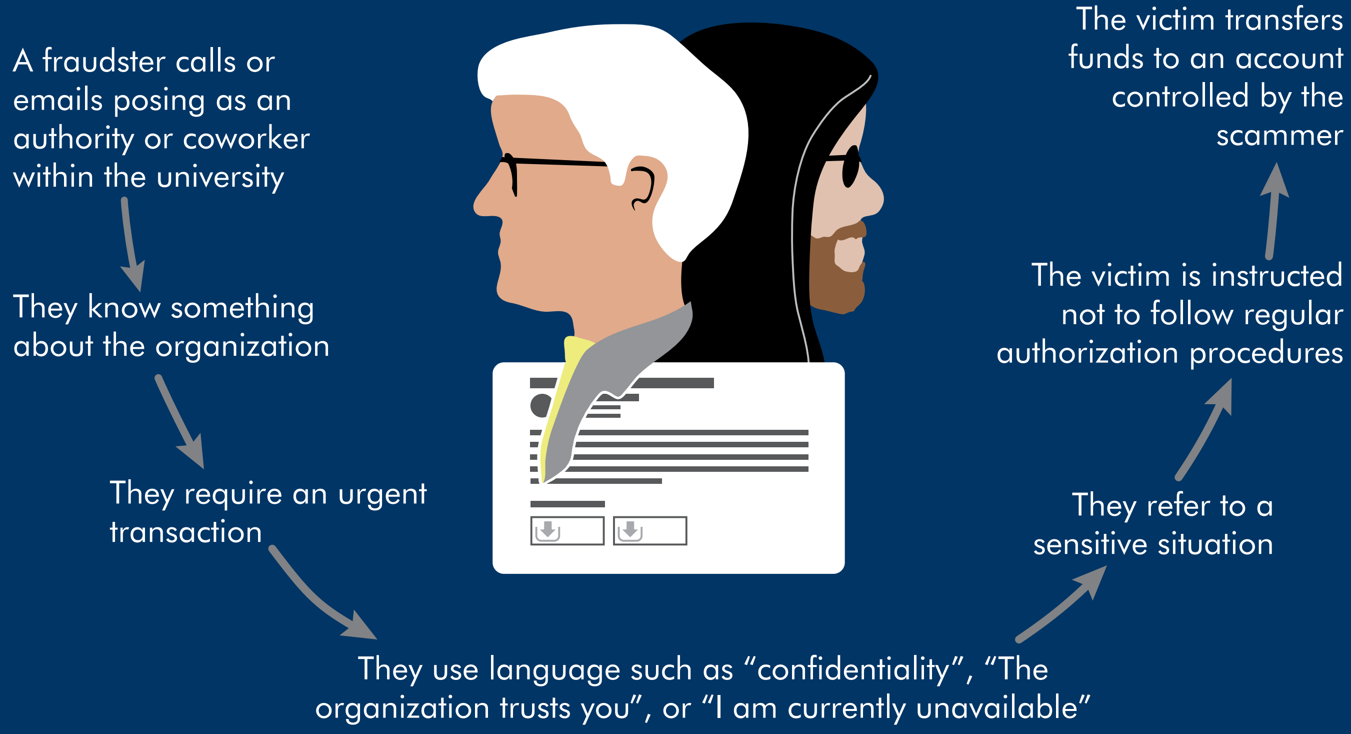
BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

IMPERSONATION FRAUD

Impersonation fraud occurs when the scammer pretends to be a trusted authority, such as a department head, manager, or even the university president, and tricks an employee authorized to make payments into paying a fake invoice or making an unauthorized transfer out of a business account.

HOW DOES IT WORK?



A fraudster calls or emails posing as an authority or coworker within the university

They know something about the organization

They require an urgent transaction

They use language such as "confidentiality", "The organization trusts you", or "I am currently unavailable"

They refer to a sensitive situation

The victim is instructed not to follow regular authorization procedures

The victim transfers funds to an account controlled by the scammer

WHAT CAN YOU DO?

Always apply payment security procedures; never skip steps, even under pressure

Always check email addresses carefully

When in doubt, consult a colleague

Never open suspicious links or attachments in emails

Avoid sharing information about your organization's structure, security, or internal procedures

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

SHOPPING SCAMS

Everyone likes finding a good deal, but sometimes online deals are too good to be true. Here's how to stay one step ahead of scams.

- **Use domestic retail websites** when possible – it will be more likely that you can sort out any problems.
- **Do your research** – check reviews before buying.
- **Use credit cards** – you have more chances of getting you money back.
- Pay only by **using a secure payment service**. Are they asking for a money transfer service or a wire transfer? Think twice!
- Pay only when connected to **a secure internet connection** – avoid using free or open public wifi.
- **Pay only on a safe device** – Keep your operating system and security software up to date.
- Beware of ads offering **outrageous deals or miracle products** – If it sounds too good to be true, it probably is!
- A pop-up ad stating you have won a prize? Think twice, you might just win malware.
- If the product doesn't arrive, **contact the seller**. If there is no answer, contact your bank.

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

GIFT CARD SCAMS

If a dean, supervisor, or coworker emails and asks you to buy gift cards, chances are, it's a fake message from a cybercriminal. Learn what to look out for; here's a common pattern:

1. Reach out

You get an unexpected message from someone who apperars to be part of your organization. Thieves can pretend to be peers by checking your organizational chart and creating a fake email address.

From: Your boss or coworker
To: You
Subject: Urgent request

Hey, are you available?

2. Request

The thief may ask you to buy, scratch, and send gift card numbers.

Could you go purchase 20 gift cards? I'd do it myself, but I'm in a meeting. I'll reimburse you later.

3. Repeat

They might try to pull the wool twice.

Thanks so much! Before you get back- I was just talking with Adam, and we actually need 20 more. Could you...?

WHAT CAN YOU DO?

- Be suspicious of any email that makes unusual requests.
- Examine the sender's email and look for unusual variations of their usual address. Sometimes a letter or number is added, or a spoofed BYU address may be used.
- Contact the sender with a trusted email address or by phone to verify unusual requests.
- If you receive a gift card message, send the email as an attachment to abuse@byu.edu
- Pass this information along to colleagues and friends

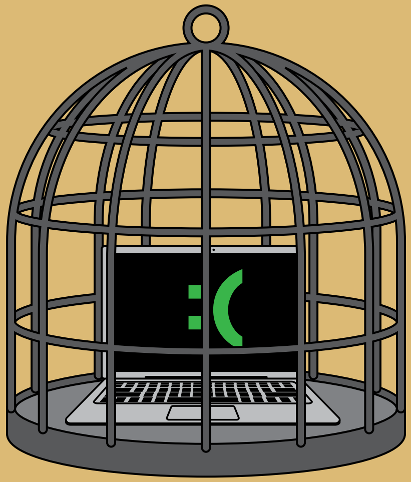
BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

RANSOMWARE

The stereotypical hacker wears a hoodie and writes viruses in his basement to crash Grandma's computer. Recently, though, hackers are targeting corporations and universities to demand large sums of money through the use of ransomware.

HOW DOES IT WORK?

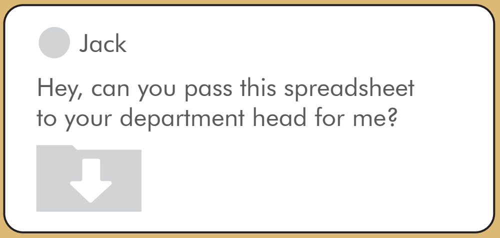


When ransomware infects a device, it encrypts the files it finds, locking the user out. The user then receives a message demanding payment which, allegedly, will grant them access to the digital key needed to unlock their files and/or system.

Ransoms may be relatively small - typically between $25 and $600 - but recent high-profile ransomware attacks have reached tens of thousands of dollars. The payment is usually collected through Bitcoin or other untraceable forms of encrypted electronic currencies, making recovery extremely difficult.

Ransomware has increased by more 97% in the past two years, costing organizations and businesses a rough average of $75 billion per year.

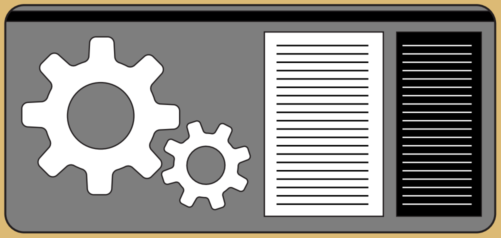
WHAT CAN YOU DO?



Jack

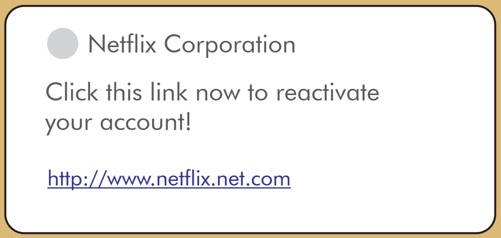
Hey, can you pass this spreadsheet to your department head for me?

Treat unexpected emails with attachments with suspicion.



Keep your software and operating systems up to date.

Set up automatic backups for your files so that you have spares in the cloud.



Netflix Corporation

Click this link now to reactivate your account!

http://www.netflix.net.com

Don't click on unfamiliar or suspicious links, even if they seem urgent.

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

INVOICE FRAUD

HOW DOES IT WORK?

Someone pretending to be a supplier, creditor, or provider approaches the university. The fraudster requests that the bank details for a recurring payment be changed to a different account. The new account in question just happens to be controlled by the fraudster.

WHAT CAN YOU DO?

- Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices.
- Do not use the contact details on the letter/fax/email requesting the change. Use those from previous correspondence instead.
- For payments over a certain threshold, set up a procedure to confirm the correct bank account and recipient (e.g. a meeting with the company).
- When an invoice is paid, send an email to inform the recipient. Include the beneficiary bank name and the last four digits of the account to ensure security.
- Set up designated Single Points of Contact with companies to whom you make regular payments.
- Restrict information that you share about your employer on social media.

BYU | OFFICE OF INFORMATION SECURITY

ONLINE SCAMS of the WORLD

JOB POSTING SCAMS

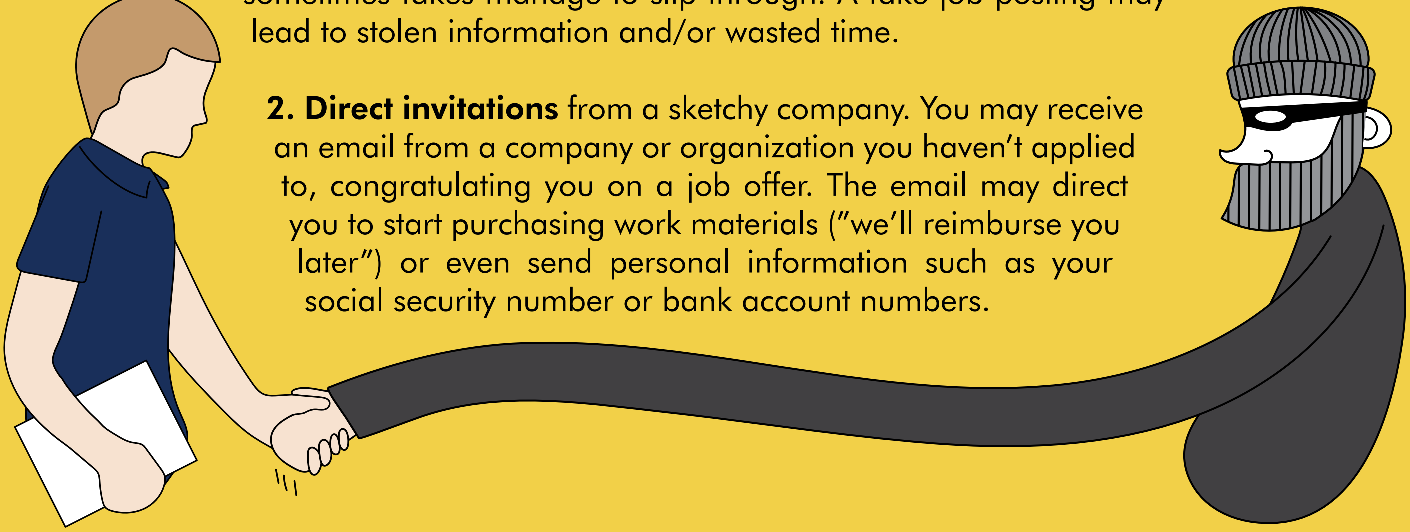
It can seem pretty daunting to get a satisfying, well-paying job right out of college. Unfortunately, scam artists know how desperate the task can make a student feel, and they're all too eager to prey on those emotions. Here's what to know so you don't fall victim to a thief or a fraudulent company.

HOW DOES IT WORK?

Job scams can come in two forms:

1. **Fraudulent postings** on a job board. Although credible sites such as Indeed, Glassdoor, and BYU's own Handshake vet job postings, sometimes fakes manage to slip through. A fake job posting may lead to stolen information and/or wasted time.

2. **Direct invitations** from a sketchy company. You may receive an email from a company or organization you haven't applied to, congratulating you on a job offer. The email may direct you to start purchasing work materials ("we'll reimburse you later") or even send personal information such as your social security number or bank account numbers.



WHAT CAN YOU DO?

- Read all about a company before applying.

- Double check the contact information a company provides. Is their office where they say it is? Do emails come from a corporate address as well?

- Don't bother with any company that asks for any deposits or fees in the application process.

- Be wary of any company that promises quick money for little work or with minimal training.

- Be suspicious of any company that seems willing to hire you without an application or an interview.

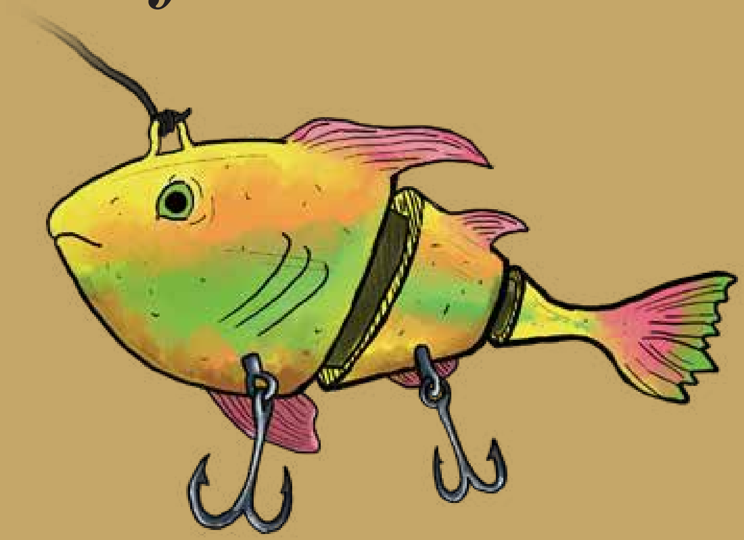
- Remember that real employers won't ask for your passwords. If they ask for your social security number and bank information, they'll do so in your first week of actual on-site work, not before.

- Contact BYU Career Services at 801.422.3000 if you have questions about a job posting.

BYU | OFFICE OF INFORMATION SECURITY

PHISHING LURES

of the world



The Deceptive Link

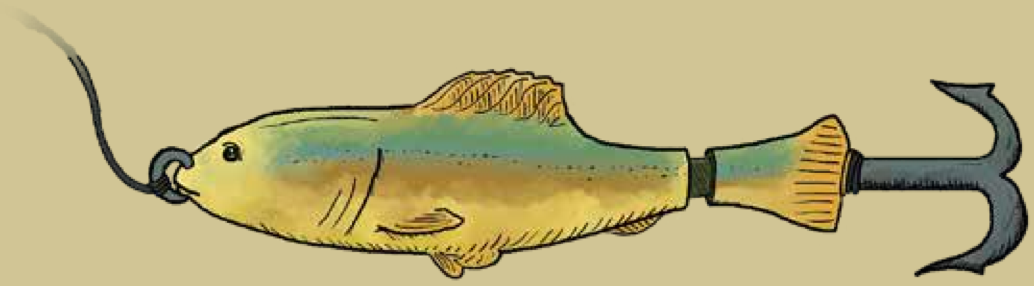
WE'RE ALL familiar with hyperlinks – the underlined blue text that whisks us in the direction of information we're looking for. Unfortunately, it's very easy to make a hyperlink say one thing, but lead to another.

IF YOU RECEIVE AN EMAIL that contains a hyperlink or button, take a single second to hover your mouse over the link. The destination URL will appear in the corner of your browser. If you're on a mobile device, press and hold the link. Just don't bother clicking until you're certain the link goes where it says it goes.

BYU | OFFICE OF INFORMATION SECURITY

PHISHING LURES

of the world



The Password Request

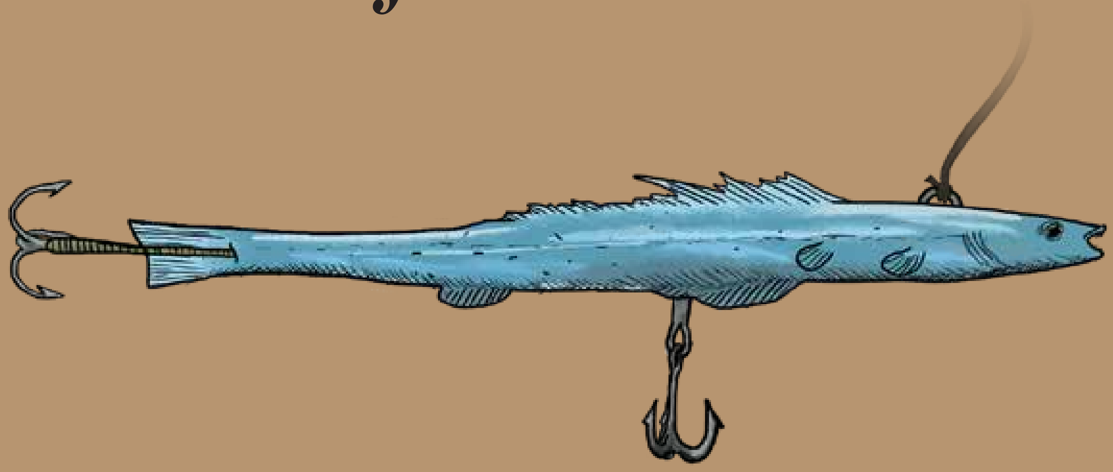
THIS LURE comes in the form of an urgent email from (what looks like) your university, your bank, or a business you have an account with. The email asks you to confirm your password because your account is “compromised”, “over quota”, or “suspended due to inactivity.”

REMEMBER, you’ll never be asked via a sudden email from a reputable organization or business for your password, SSN, or other private identifying information. If someone makes this kind of request of you in an email, report the sender to abuse.byu.edu.

BYU | OFFICE OF INFORMATION SECURITY

PHISHING LURES

of the world



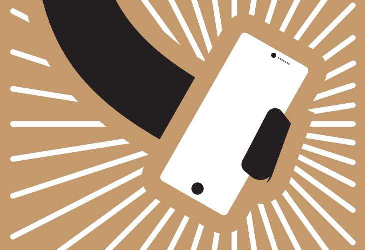
The Unexpected File

ON A DAY when you aren't expecting it, you find an email in your inbox with an attached file. It may appear to be from your school, an old subscription service, or even a manager or friend. The email sounds urgent - open the file now, or something bad could happen!

DON'T BE FOOLED. It's okay to be skeptical of emails you weren't anticipating, and it's doubly okay to take your time in verifying the sender. Identity thieves and hackers want you to act quickly; reputable organizations, on the other hand, won't use fear or pressure to convince you to act.

BYU | OFFICE OF INFORMATION SECURITY

PROTECT YOUR IDENTITY



YOUR PROFILES

Your personal brand shouldn't compromise your identity. Limit what you share on social media and don't grant third-party apps access to your profile.

YOUR DEVICES

Make sure your devices' software is always up to date, and be very careful when using public WiFi.

YOUR PASSWORD

Use long passwords. Make sure each of your accounts has a unique password. Use a 2-factor system, such as Duo, whenever possible.

YOUR CLOUD

Back up important files to a secure, encrypted cloud service like OneDrive, Google Docs, or Box.

YOUR EMAIL

Be vigilant for phishing attempts. Never give out your sensitive information or passwords, and don't click on links in suspicious emails. Forward phishing emails to abuse@byu.edu

YOUR FINANCES

Only do your online shopping on secure sites and secure networks (not public ones). Look for "https://" in the address bar.

BYU | OFFICE OF INFORMATION SECURITY

HOW DO YOU KNOW IF YOU'VE BEEN hacked?

YOUR FRIENDS TELL YOU

They've received a spammy or phishy e-mail from your email account, social media, messaging apps, or SMS.

YOUR BROWSER TELLS YOU

Unwanted browser toolbars, homepages, or plugins appear unexpectedly. You're seeing lots of pop-ups or web page redirects. Your online passwords don't work.

YOUR PHONE TELLS YOU

Battery and data usage are higher than normal. Charges for premium SMS numbers show up on your bill.

YOUR EMAIL TELLS YOU

You receive a notification from a company that has recently suffered a cybersecurity breach.

YOUR BANK TELLS YOU

You receive collection calls. There's money missing from your bank account. You get messages and receipts for things you didn't buy.

YOUR SOFTWARE TELLS YOU

New accounts appear on your device. Your antivirus software pulls up red alerts. You get messages from software you don't recall installing. Programs crash randomly.

BYU | OFFICE OF INFORMATION SECURITY